ProxyServer
Internet Access / Firewall

Dual Ethernet ProxyServer

Model MTPSR1-120

User Guide

MultiTech® Systems

User Guide

S0000011 Revision C

Dual Ethernet ProxyServer (Model MTPSR1-120)

This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved.

Copyright © 2000, by Multi-Tech Systems, Inc.

Multi-Tech Systems, Inc. makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Record of Revisions

Revision	Description
A (9/4/98)	Manual released. All pages at revision A.
B (2/19/99)	Manual revised for software version 2.00. All pages at Revision B.
C (2/15/2000)	Manual revised for software version 3.00. All pages at Revision C.

Patents

This Product is covered by one or more of the following U.S. Patent Numbers: ***5.301.274; 5.309.562***; ***5.355.365; 5.355.653; 5.452.289; 5.453.986***. Other Patents Pending.

TRADEMARK

Trademark of Multi-Tech Systems, Inc. is the Multi-Tech logo.
Windows is a registered trademark of Microsoft.

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(763) 785-3500 or (800) 328-9717
Fax 763-785-9874
Tech Support (800) 972-2439
Internet Address: http://www.multitech.com

Contents

Chapter 1 - Introduction and Description

Introduction 6
Preview of this Guide 6
Front Panel Description 8
Back Panel Description 9
- RS232/V.35 Connector 9
- Ethernet 1 and 2 10Base-T Connectors 9
- Command Connector 9
- Power Connector 9

Typical Applications 10
- Configuration 1 - Cable/DSL Modem 10
- Configuration 2 - Existing Dual-LAN with Router 11
- Configuration 3 - New Dual-LAN with T1 DSU 12

Specifications 13
- Ethernet Ports 13
- Command Port 13
- WAN Link 13
- Electrical/Physical 13

Chapter 2 - Installation

Safety Warnings 16
Unpacking Your Firewall 16
V.35 Shunt Procedure 17
Cabling Your Firewall 18

Chapter 3 - Software Loading and Configuration

Loading your Software 22
- Wizard Setup 24
- IP Wizard Setup 25

Default WAN Link Configuration 27

Chapter 4 - Firewall Software

Introduction 30
- Before You Begin 30

Firewall Setup 31
Changing IP Parameters 32
Changing PPP/SLIP Parameters 35
Changing WAN Port Parameters 35
Enabling the DHCP Server 37
Adding Proxy Applications 38
Adding Virtual Servers 40
Managing Various Applications 43
Running Statistics 44
User - Filter Management 45
- User Management 46
- Access Rights 47

User Monitoring 48

Chapter 5 - Client Setup

Introduction 50
Before you Begin 50
Configuring in Windows 98/95 51
Installing TCP/IP (Win98/95) 58
Configuring in Windows NT 59
Installing TCP/IP (WinNT) 65

Chapter 6 - Remote Configuration

Introduction 68
Remote Configuration 68
    Modem-based 68
    LAN-based 70

Chapter 7 - Firewall Management

Introduction 74
Firewall Management Menu 75
Web Browser Management 76

Chapter 8 - Warranty, Service and Tech Support

Introduction 80
Limited Warranty 80
    On-line Warranty Registration 80
Tech Support 81
    Recording Firewall Information 81
Service 82
About the Internet 83
Ordering Accessories 83

Appendixes

Appendix A - TCP/IP (Transmission Control Protocol/Internet Protocol) Description 86
Appendix B - Cabling Diagrams 89
Appendix C - Script Commands 91
Appendix C - Regulatory Information 93
    FCC Declaration 93

Glossary of Terms

Index

ProxyServer
Internet Access / Firewall

Chapter 1 - Introduction and Description

MultiTech® Systems

Introduction

Welcome to Multi-Tech's new Dual Ethernet ProxyServer, model MTPSR1-120, (hereafter, Firewall) a high speed Internet access device that provides firewall protection to your corporate (secured) LAN and allows Internet access to the Internet Services Network (public LAN) that resides outside the firewall. Internet access can be provided through new technologies, such as cable or DSL modems, connecting to an existing high speed public LAN, or connecting the RS232 WAN port on the back of the unit that allows Internet access up to T1/E1 access speeds. The Firewall provides two Ethernet connections that implement firewall protection and gateway security for your LAN resources and provides megabit data transfer rates (up to 20 times faster than a 56K modem) for your Internet access.

The Firewall provides two Ethernet 10Base-T ports which connect your private secured LAN (on the **Ethernet 1** jack) to the Internet Services Network resources (public LAN, on the **Ethernet 2** jack), and a Command port for configuration. An additional RS232/V.35 port is provided for an alternate connection to an external WAN for connecting your secure corporate LAN directly to an ISP.

System management is provided through the command port using bundled Windows® software which provides easy-to-use configuration menus.

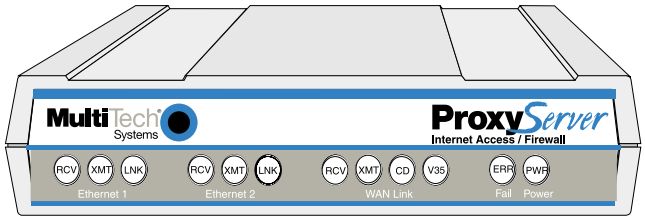


Figure 1-1. Firewall (MTPSR1-120)

Preview of this Guide

This guide describes the Firewall and tells you how to install and configure the unit. The information contained in each chapter is as follows:

Chapter 1 - Introduction and Description

Chapter 1 describes the Firewall's front panel indicators and back panel connectors and switch, and includes a list of relevant specifications.

Chapter 2 - Installation

Chapter 2 provides information on unpacking and cabling your Firewall. The installation procedure describes each cable connection.

Cabling considerations involve deciding how you are going to connect your PC to the Firewall to configure it for proper operation in your system. One option is to connect a PC COM port (1 thru 4) through the supplied command cable to the COMMAND port on the Firewall. The other option is to connect your PC's network interface card (NIC) to a hub on your Private LAN and connect the ETHERNET 1 jack of the Firewall to your Private LAN and then assign the Firewall an IP address on your Private LAN. During software installation, the Firewall will detect automatically *all* Firewalls and ProxyServers on the LAN and will let you select which one to configure.

Your final cabling consideration involves deciding which back panel connector you will use to connect your Private (secured) LAN to the Internet. Your options include the ETHERNET 2 LAN jack or the RS233/V.35 WAN connector; only one Ethernet connection method can be used.

Chapter 3 - Software Loading and Configuration

Chapter 3 provides instructions for software loading and initial configuration. The Firewall CD ROM is Windows® based. Later chapters, as well as the included on-line Helps, describe the Firewall software in greater detail.

Chapter 4 - Firewall Software

Chapter 4 describes the Firewall software package designed for the Windows ® environment. The Firewall Version 3.00 program group includes icons for performing such functions as Wizard Setup, downloading firmware, Configuration port setup, WAN Device Configuration, etc. Fields on dialog boxes are explained in detail and when fields relate to each other, that relationship is explained.

Chapter 5 - Client Setup

Chapter 5 provides information for enabling and configuring multiple Windows 98/95 or NT® PC users for Internet access via the Firewall.

Chapter 6 - Remote Configuration

Chapter 6 provides procedures for changing the configuration of a remote Firewall. Using remote configuration, you can change the configuration of a remote unit by simply connecting two modems between the Firewalls (with a special remote configuration cable between the remote modem and the remote Firewall's command port) and remotely controlling the remote unit.

Chapter 7 - Firewall Management

Chapter 7 discusses remote management utilities such as Telnet and Web-based management of the Firewall.

Chapter 8 - Warranty, Service and Tech Support

Chapter 8 provides instructions on getting service for your Firewall at the factory, a statement of the limited warranty, information about our Internet presence, and space for recording information about your Firewall prior to calling Multi-Tech's Technical Support.

Appendixes

Appendix A - TCP/IP (Transmission Control Protocol/Internet Protocol) Description

Appendix B - Cabling Diagrams

Appendix C - Regulatory Information

Front Panel Description

The front panel, shown in Figure 1-2, contains four groups of LEDs that provide the status of the Ethernet connections, WAN link activity, and general status of the Firewall. The Ethernet 1 and Ethernet 2 LEDs display the activity of the public and private LANs, and show if the Firewall is connected to the LAN and transmitting or receiving packets. The WAN Link LEDs display the status of the RS232/V.35 WAN link, that can optionally be connected to an external DCE device, and show if a carrier signal is detected, if the link is ready to transmit or receive serial data, and if an external communications device with a V.35 interface is connected to the Firewall. The last group of LEDs indicates whether the self test passed or failed and shows if the power On/Off switch on the back of the Firewall is turned On.

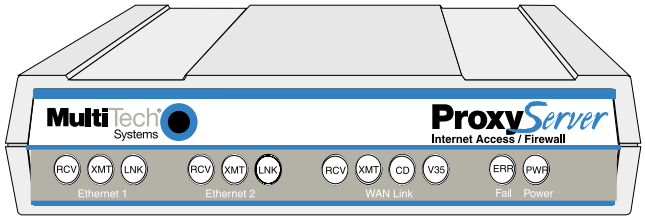


Figure 1-2. Front Panel

ETHERNET 1 and 2

RCV Receive Data indicator blinks when packets are being received from the private (Ethernet 1) or public (Ethernet 2) LANs.

XMT Transmit Data indicator blinks when packets are being transmitted to the private (Ethernet 1) or public (Ethernet 2) LANs.

LNK Link indicator lights when the Ethernet link senses voltage from a concentrator or external device.

WAN Link

RCV Receive Data indicator blinks when packets are being sent to the local area network.

XMT Transmit Data indicator blinks when packets are being transmitted from the local area network.

CD Carrier Detect indicator lights when a carrier signal is detected on the WAN link.

V35 V.35 indicator lights when internal shunt is set for V.35 operation.

Fail

ERR Error indicator lights when the Firewall is booting or downloading setup.

Power

PWR Power indicator lights when power is applied to the Firewall.

Back Panel Description

All the cable connections for the Firewall are made at the back panel. In addition to the Power connector, three other categories of connectors are used on the Firewall: the Command Port, Ethernet 1 & 2 (10BASET), and RS232/V.35. The back panel connectors are shown in Figure 1-3 and defined in the following writeups.

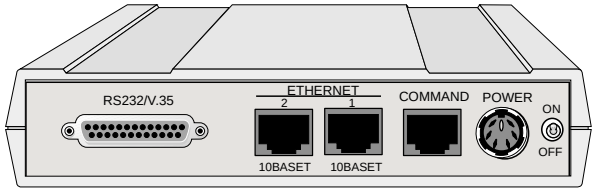


Figure 1-3. Back Panel

RS232/V.35 Connector

The RS232/V.35 (DB-25) connector is used to connect the Firewall to an external modem, DSU, or other Data Communications Equipment (DCE). This connection can be either RS232C (default) or V.35. If the connection is V.35, then the shunt must be moved from the default RS232 position to the V.35 position (for details on this procedure, refer to Chapter 2 - V.35 Shunt Procedure).

Ethernet 1 and 2 10Base-T Connectors

The Ethernet 10Base-T connectors are used to connect the Firewall to a 10 MB LAN using unshielded twisted cable. Ethernet 1 connects the private LAN, and Ethernet 2 connects the public LAN. These connectors are RJ-45 jacks.

Command Connector

The Command connector is used to configure the Firewall using a PC with a serial port and running Windows® software. The Command connector is an RJ-45 jack and a short adapter cable is provided to convert to a standard serial port DB-9 female connector.

Power Connector

The Power connector is used to connect the external power supply to the Firewall. The Power connector is a 6-pin circular DIN connector. A separate power cord is connected between the power supply and a live AC grounded outlet.

Typical Applications

This section describes three typical applications and assumes that the Firewall will be configured for a particular application during the initial installation. Each example includes a detailed system-type diagram.

In the first of these applications, the Firewall connects a private LAN to the Internet through a cable modem or a Digital Subscriber Line (DSL) modem, thus providing high speed Internet access. The second application ties a private LAN and public Internet Services Network (e.g., an existing public LAN) through its router to the Internet. The third application is similar to the second, but uses a Data Communications Equipment (DCE) device—in this example, a T1 DSU—connected to the RS232 port on the back panel of the Firewall to connect to the Internet.

Configuration 1 - Cable/DSL Modem

In Figure 1-1, a private LAN is connected to the **ETHERNET 1** jack on the back panel of the Firewall. Internet access is provided through a cable modem or DSL modem that is connected to the **ETHERNET 2** jack on the Firewall.

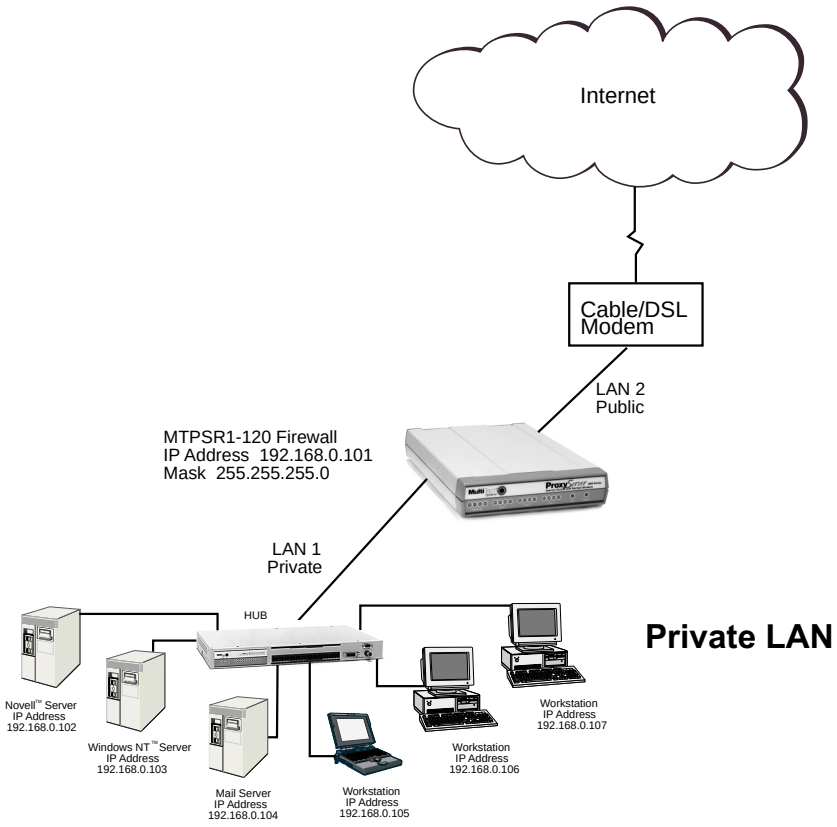


Figure 1-1. Cable/DSL Modem Configuration

When the Firewall software is loaded, the Secured LAN Port Parameters are configured to include an unregistered IP Address and associated Net Mask for the private LAN (on ETHERNET 1). Then, the Internet LAN Port Parameters are configured with the DHCP Client option active. This enables the Internet Services Provider (ISP) to dynamically provide the registered Internet IP addresses at each login. (If a static IP addressing scheme is provided by the ISP, then the assigned static IP address is used instead.)

Configuration 2 - Existing Dual-LAN with Router

Another typical configuration, shown in Figure 1-2, ties a private LAN (on ETHERNET 1) to an existing Internet Services Network already providing Internet services. This configuration provides firewall and gateway security for the LAN users, and supports Internet access restrictions based on IP addresses, domain names, applications, client protocols, or lists of forbidden (or allowed) sites.

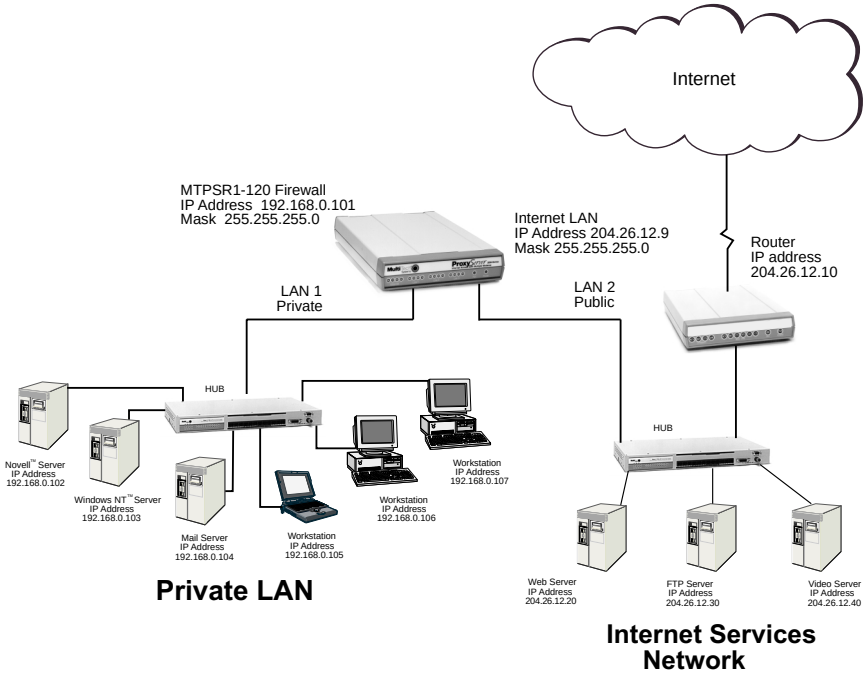


Figure 1-2. Existing Dual-LAN with Router Configuration

In Figure 1-2, the private LAN is again connected to the **ETHERNET 1** jack on the back panel of the Firewall. The Internet Services Network, or public LAN, is connected to the **ETHERNET 2** jack. Access to the Internet is provided by the existing router connected to the Internet Services Network.

Configuration 3 - New Dual-LAN with T1 DSU

The final typical configuration, shown in Figure 1-3, brings Internet access to existing LAN users. With this configuration, the private LAN (on ETHERNET 1) is secured by the firewall while the Internet Services Network is outside the firewall enabling Internet users to access (through ETHERNET 2) the public LAN resources, such as the Web, FTP, etc. servers. In this arrangement, the Internet connection is provided through a T1 DSU connected to the RS232/V.35 connector on the back panel of the Firewall.

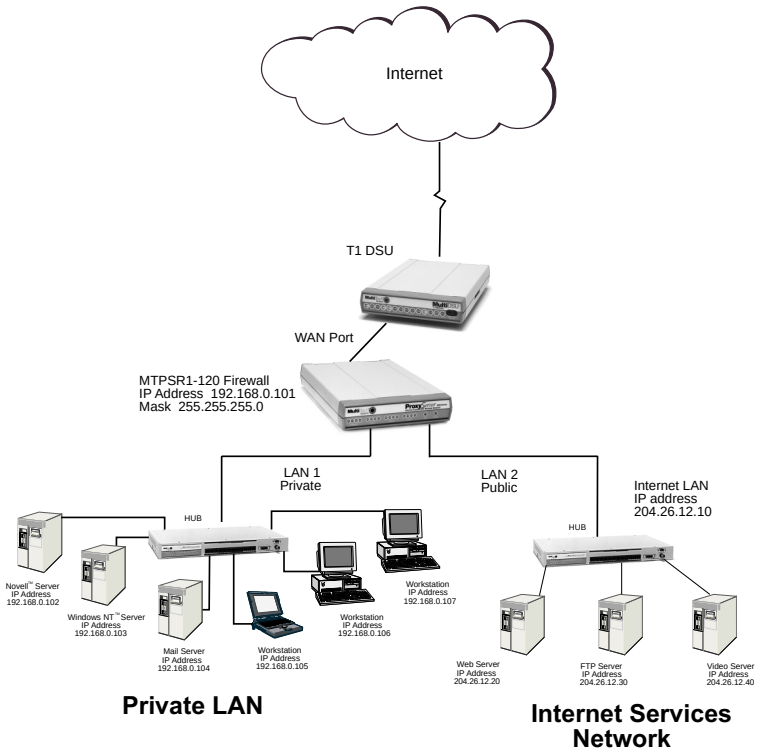


Figure 1-3. New Dual-LAN with T1 DSU Configuration

In addition to setting up the Secured LAN Port and Internet LAN Port parameters (as above), the user must also enable the WAN port and enter the phone number for the ISP and the user name and password agreed upon with the ISP.

Specifications

- Protocols - Point-To-Point Protocol (PPP), and Serial Line Internet Protocol (SLIP)

Ethernet Ports

- Two Ethernet Interfaces - 10Base-T (twisted pair) RJ-45 jacks

Command Port

- Single 19.2K bps asynchronous Command Port using an RJ-45 to DB-9 (female) cable

WAN Link

- One RS232/V.35 port connector (DB-25 female)

Electrical/Physical

- Voltage - 115 VAC (Standard), 240 Volts AC (Optional)
- Frequency - 47 to 63 Hz
- Power Consumption - 10 Watts
- Dimensions - 1.625" high x 6" wide x 9" deep

  5.63 cm high x 22.34 cm wide x 22.34 cm deep
- Weight - 2 pounds (.92 kg)

ProxyServer
Internet Access / Firewall

Chapter 2 - Installation

MultiTech® Systems

Safety Warnings

1. Never install phone wiring during a lightning storm.
2. Never install phone jacks in wet locations unless the jack is specifically designed for wet locations.
3. This product is to be used with UL and cUL listed computers.
4. Never touch uninsulated phone wires or terminals unless the phone line has been disconnected at the network interface.
5. Use caution when installing or modifying phone lines.
6. Avoid using a phone (other than a cordless type) during an electrical storm. There may be a remote risk of electrical shock from lightning.
7. Do not use the phone to report a gas leak in the vicinity of the leak.
8. To reduce the risk of fire, use only No. 26 AWG or larger Telecommunication line cord.

Unpacking Your Firewall

The shipping box contains the Firewall, external power supply, power cord, Command Port (RJ-45 to DB-9) cable, your Quick Start Guide, and a CD ROM with the Firewall Software and the Firewall User Guide. Inspect the contents for signs of any shipping damage. If damage is observed, do not power up the unit, contact Multi-Tech's Technical Support for advice (refer to Chapter 8). If no damage is observed, place the Firewall in its final location and continue with the next section.

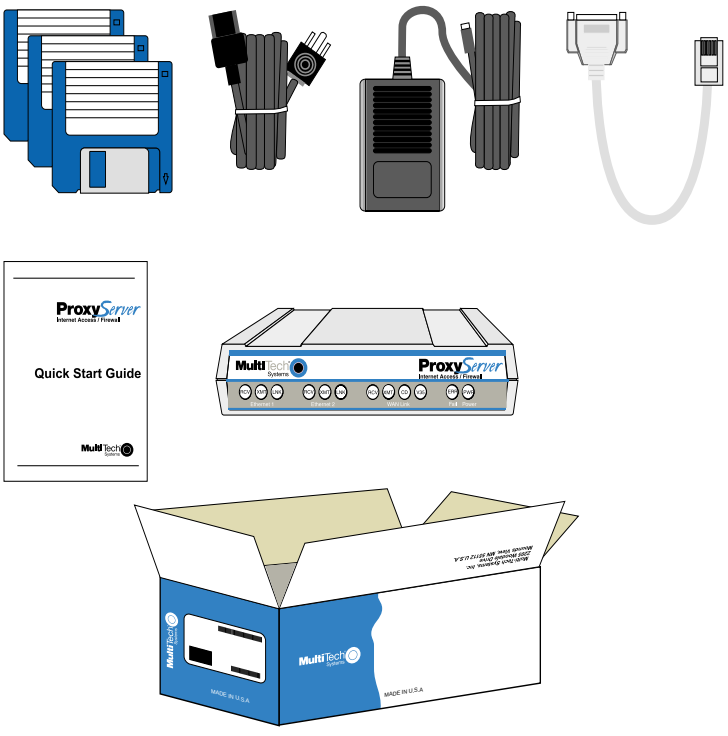


Figure 2-1. Unpacking Your Firewall

V.35 Shunt Procedure

If you are using an external DCE device on the WAN RS232/V.35 port, and the connection will be a V.35 connection, the internal shunt must be moved from the RS232C (default) position prior to cabling and power-up. The following steps detail the procedures for switching the shunt.

1. Ensure that the external power supply is disconnected from the Firewall.
2. Turn the Firewall over and remove the cabinet mounting screw from the chassis.

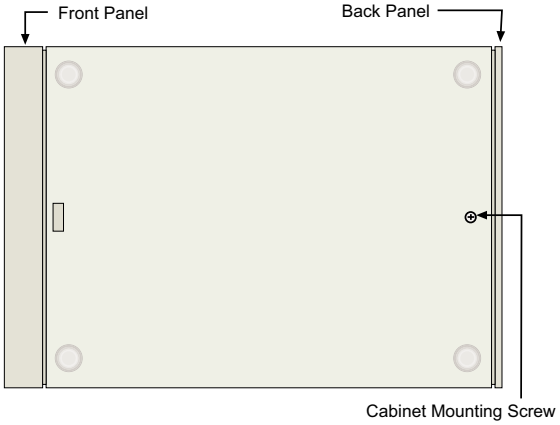


Figure 2-2. Cabinet Mounting Screw

3. While supporting the back panel, turn the Firewall right side up, tilt the back panel down, and slide the circuit board assembly out of the chassis.
4. Place the circuit board assembly on a flat, grounded surface.
5. Carefully remove the shunt from the RS232 position, and insert it in the V.35 position (Figure 2-3).

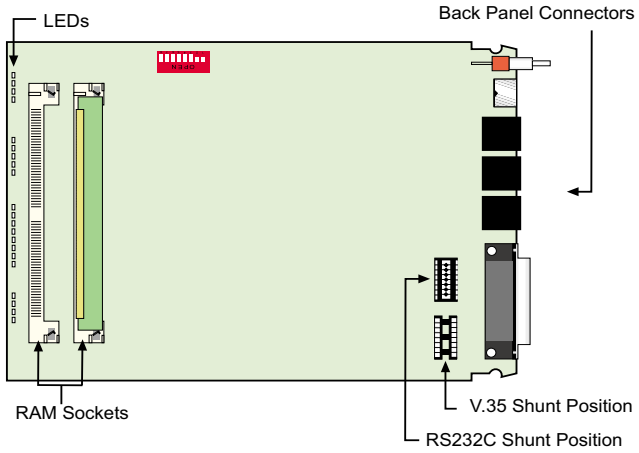


Figure 2-3. Shunt Positions

6. Align the board with the guide slots on the inside of the chassis and carefully slide the board back into the chassis.
7. While supporting the back panel, turn the Firewall over again, and replace the cabinet mounting screw.
8. Turn the Firewall right side up again and proceed to the next section to connect the cables.

Cabling Your Firewall

Cabling your Firewall involves making the proper Power, Command Port, and two Ethernet connections. An optional WAN connection is provided to connect to an external WAN device.

Before connecting cables to your Firewall, consider the following cabling alternatives:

1. Will you be configuring the Firewall from your PC via the command cable as shown in Figure 2-4, or will you use an existing network connection over your Private (secure) LAN?

   Note: Initial configuration of the Firewall cannot be done over The Web; however, the initial configuration can be “edited” (reconfigured) later over The Web.

2. How will you connect your Firewall to your Private (secure) LAN?

3. Will you connect to the Internet over an existing Public LAN, or will you use the RS232/V.35 WAN connection on the back panel of the Firewall?

Figure 2-4 shows the back panel connectors and the associated cable connections, and the procedure that follows details the steps for connecting the cables to your Firewall.

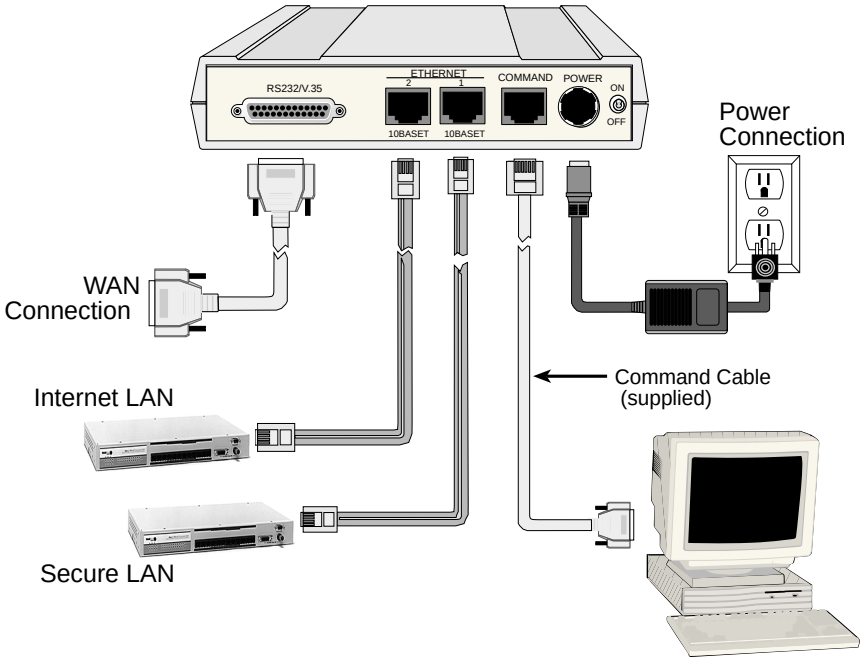


Figure 2-4. Cable Connections

1. With the ON/OFF switch set to **OFF**, connect one end of the power supply to a live AC outlet and connect the other end to the Firewall as shown in Figure 2-4. The power connector is a 6-pin circular DIN connector.
2. To configure the Firewall through the Command port, use the special RJ-45 to DB-9 (female) command cable packed with your unit. Plug the RJ-45 end of the cable into the Command port of the Firewall and the other end into the PC COM port you are using. See Figure 2-4.

   Alternate: You can configure your Firewall from a PC connected to your Secure LAN.
3. To connect your secure (private) LAN, connect one end of an RJ-45 (UTP) cable to the ETHERNET 1 jack on the back panel of the Firewall. Connect the other end of the cable to a hub on your private LAN.

   Note: Your Internet connection can be made through *either* the **ETHERNET 2** port (step 4) or the **RS232/V.35** connector (step 5); however, only one of these ports can be used at a time.

4. To connect a cable modem, DSL modem, or your Internet (public) LAN, connect one end of an RJ-45 (UTP) cable to the ETHERNET 2 jack on the back of the Firewall; then connect the other end to your modem or Internet LAN. Proceed to step 6.
5. If you connected a cable modem, DSL modem, or your Internet LAN in the previous step, do not connect anything to the RS232/V.35 connector on the back of the Firewall. However, if the RS232/V.35 connector on the Firewall is going to be connected to a WAN device (i.e., connecting your secure (private) LAN to an ISP, connect one end of an RS232 or V.35 interface cable to the RS232/V.35 connector on the back of the Firewall. Connect the other end of this cable to the WAN device.
6. Apply power to the Firewall by setting the ON/OFF switch on the back panel to the ON position. **Wait** for the Fail LED on the Firewall to go Off before proceeding. This may take a couple of minutes to go Off.

   At this time your Firewall is completely cabled and powered. Proceed to Chapter 3 to load the Firewall software.

ProxyServer
Internet Access / Firewall

Chapter 3 - Software Loading and Configuration

MultiTech® Systems

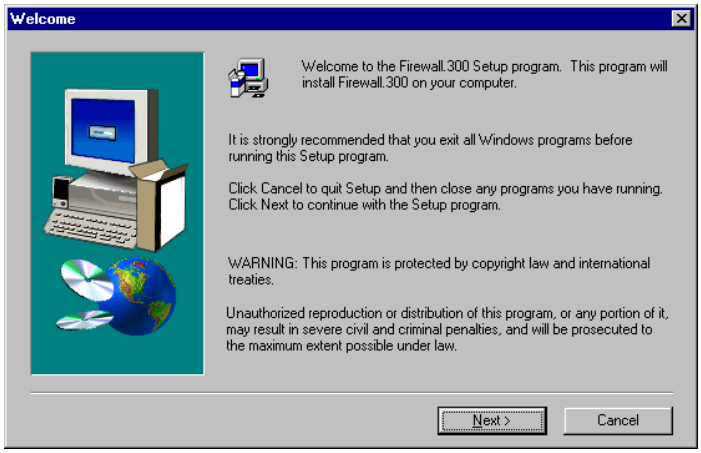
Loading your Software

The following procedure for software installation and initial configuration does not provide every screen or option in the process of installing the Firewall software. The assumption is that a technical person with a thorough knowledge of Windows and the software loading process is doing the installation and configuration. Additional information on the Firewall software is provided in Chapter 4, Firewall Software.

1. Before inserting the Firewall CD-ROM into your CD-ROM drive, determine whether you will configure your Firewall over the LAN or directly from a COM port of a local PC. For configuring over a network, your PC must first be configured for network communications (i.e., TCP/IP stack must be installed) and both the PC and the Firewall must be on the same physical LAN segment. If you need to load the TCP/IP stack, refer to Chapter 5, Client Setup.
2. Insert the Firewall CD-ROM into the CD-ROM drive on your local PC. The CD-ROM should start automatically; however, it may take 10 to 20 seconds for the Multi-Tech Installation CD screen to appear.

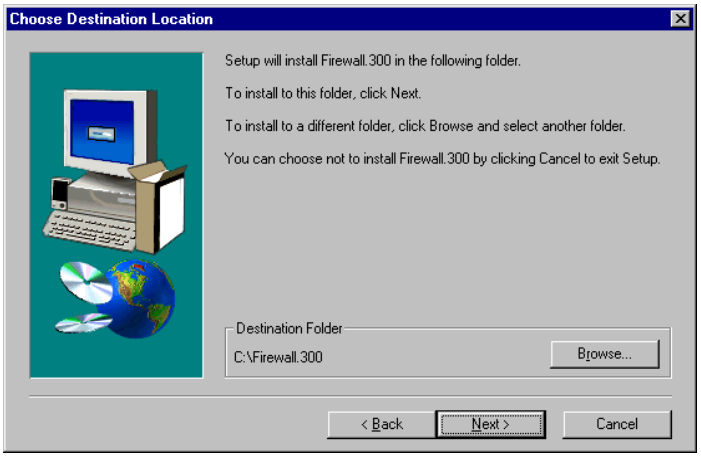
If the Multi-Tech Installation CD Screen does not appear automatically, click **My Computer**, then right-click the **CD-ROM drive** icon and click **Autorun**.

3. When the Multi-Tech Installation CD Screen appears, click the **Install Software** icon.
4. The Welcome screen is displayed.


Welcome
Welcome to the Firewall.300 Setup program. This program will install Firewall.300 on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Next >
Cancel

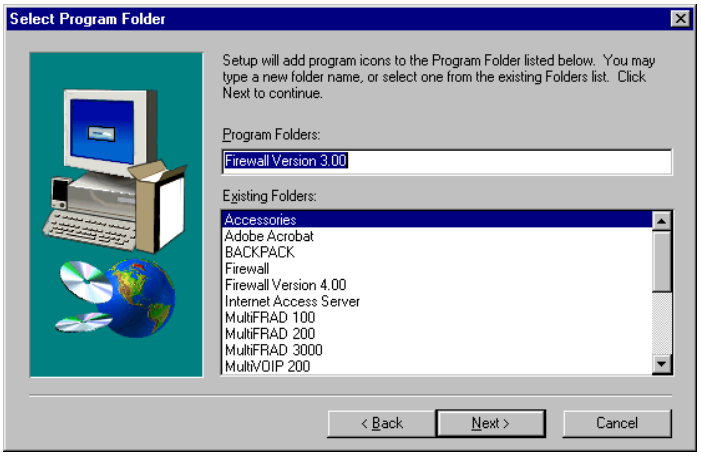
Click **Next >** or press **Enter** to continue.

5. The **Choose Destination Location** dialog box is displayed. Follow the onscreen instructions to install your Firewall 3.00 software.


Choose Destination Location
Setup will install Firewall.300 in the following folder.
To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
You can choose not to install Firewall.300 by clicking Cancel to exit Setup.
Destination Folder
C:\Firewall.300
Browse...
< Back
Next >
Cancel

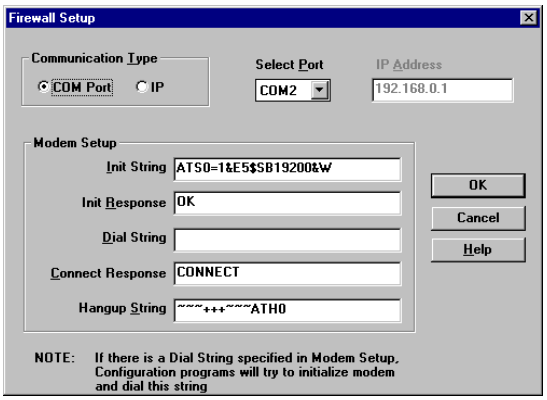
You can either choose a different Destination Location of your Firewall 3.00 software by clicking **Browse**, or select the default destination by pressing **Enter** or clicking **Next>**. It is recommended that you accept the default folder, **C:\Firewall.300**.

6. The **Select Program Folder** dialog box enables you to name the program group for the Firewall 3.00 icons. You can either select the default name, **Firewall Version 3.00**, or name it anything you like.



Click **Next>** or press **Enter** to continue.

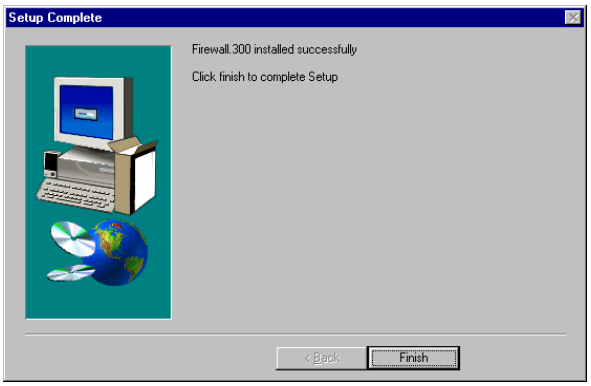
7. The next dialog box enables you to designate the COM port of your PC that is connected to the Firewall. On the **Select Port** field, click the down arrow and select the COM port (COM1 -- COM4) that is connected to the Firewall.



Click **OK** to continue.

If you need to configure your Firewall through the COM port, follow the instructions in the dialog box for selecting **COM Port**, then click **OK** to continue.

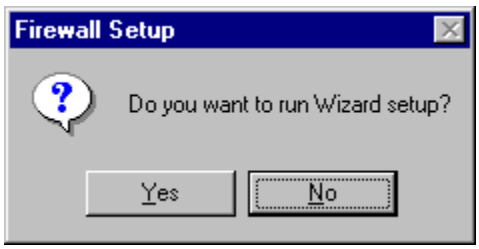
8. The software is loaded onto your PC, then the **Setup Complete** dialog box is displayed.



Click **Finish** to continue. The “Do you want to run Wizard setup?” message is displayed.

Wizard Setup

The Wizard Setup screen gives you a process for adding the basic information needed to configure your Firewall. This screen will guide you through entering the IP Address, Net Mask, and Default Route for your Secure (private) LAN. Then you can set up for static or dynamic addressing on the Internet LAN Port, set up the Gateway Parameters, and then do the same for the WAN port, if it is used.



9. Click **Yes** to run the Wizard Setup.

   Clicking **No** takes you to the program group (icons), where you can choose a utility from the program group.

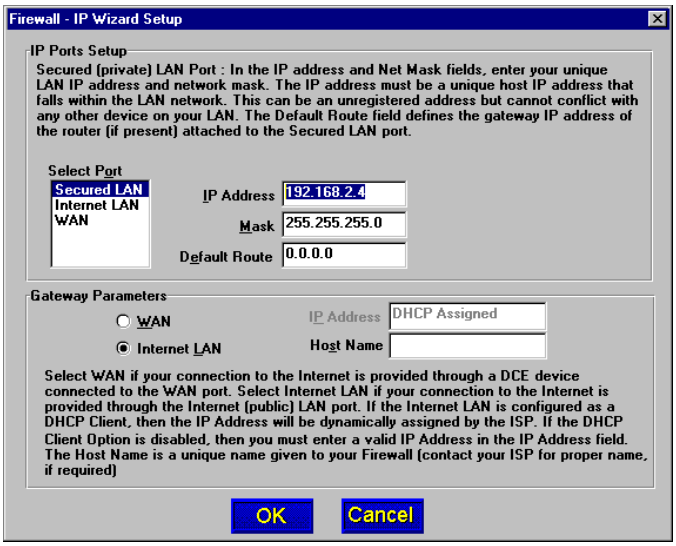
IP Wizard Setup

The IP Wizard Setup dialog box guides you through assigning LAN and WAN IP address information. If the configuration type is set to IP, the IP Wizard will attempt to automatically detect all Firewalls on your Secure (private) LAN.

10. Change the default IP Address, Mask, and Default Route to the unique parameters for your Secure (private) LAN connected to the ETHERNET 1 Port.

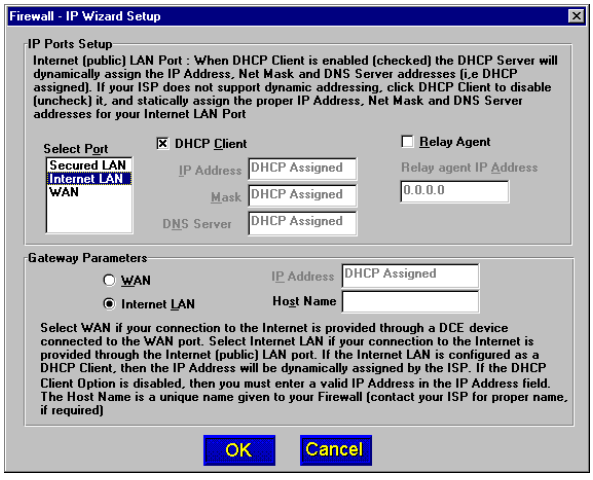
    Follow the onscreen instructions.

Secured LAN (ETHERNET 1) Setup


Firewall - IP Wizard Setup
IP Ports Setup
Secured (private) LAN Port : In the IP address and Net Mask fields, enter your unique LAN IP address and network mask. The IP address must be a unique host IP address that falls within the LAN network. This can be an unregistered address but cannot conflict with any other device on your LAN. The Default Route field defines the gateway IP address of the router (if present) attached to the Secured LAN port.
Select Port
Secured LAN
Internet LAN
WAN
IP Address
192.168.2.4
Mask
255.255.255.0
Default Route
0.0.0.0
Gateway Parameters
WAN
Internet LAN
IP Address
DHCP Assigned
Host Name
Select WAN if your connection to the Internet is provided through a DCE device connected to the WAN port. Select Internet LAN if your connection to the Internet is provided through the Internet (public) LAN port. If the Internet LAN is configured as a DHCP Client, then the IP Address will be dynamically assigned by the ISP. If the DHCP Client Option is disabled, then you must enter a valid IP Address in the IP Address field. The Host Name is a unique name given to your Firewall (contact your ISP for proper name, if required)
OK
Cancel

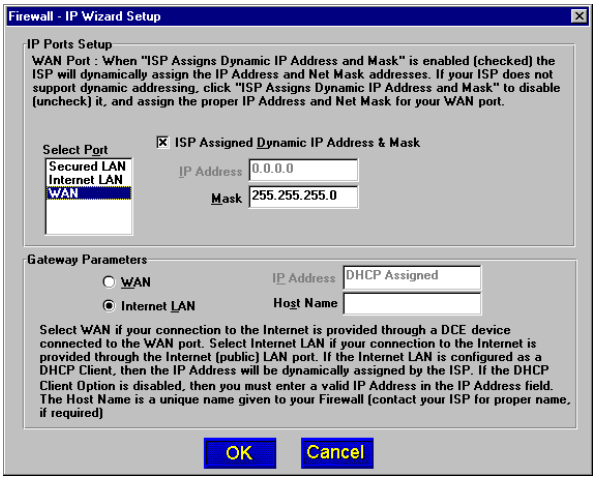
11. If an Internet (public) LAN is connected to the ETHERNET 2 Port, click the **Internet LAN** option in the **Select Port** window, then either leave the **DHCP Client** option enabled or disable (uncheck) it and assign the proper IP Address, Net Mask, and DNS Server addresses for your Internet LAN. Follow the onscreen instructions and enter a Gateway IP Address, too, if the DHCP function is disabled.

Internet LAN (ETHERNET 2) Setup


Firewall - IP Wizard Setup
IP Ports Setup
Internet (public) LAN Port : When DHCP Client is enabled (checked) the DHCP Server will dynamically assign the IP Address, Net Mask and DNS Server addresses (i.e DHCP assigned). If your ISP does not support dynamic addressing, click DHCP Client to disable (uncheck) it, and statically assign the proper IP Address, Net Mask and DNS Server addresses for your Internet LAN Port
Select Port
Secured LAN
Internet LAN
WAN
DHCP Client
Relay Agent
IP Address
DHCP Assigned
Mask
DHCP Assigned
DNS Server
DHCP Assigned
Relay agent IP Address
0.0.0.0
Gateway Parameters
WAN
Internet LAN
IP Address
DHCP Assigned
Host Name
Select WAN if your connection to the Internet is provided through a DCE device connected to the WAN port. Select Internet LAN if your connection to the Internet is provided through the Internet (public) LAN port. If the Internet LAN is configured as a DHCP Client, then the IP Address will be dynamically assigned by the ISP. If the DHCP Client Option is disabled, then you must enter a valid IP Address in the IP Address field. The Host Name is a unique name given to your Firewall (contact your ISP for proper name, if required)
OK
Cancel

WAN Setup

12. If a WAN device is connected to the WAN Port (marked **RS-232/V.35**), click the **WAN** option in the **Select Port** window, then either leave the **"ISP Assigned Dynamic IP Address & Mask"** option enabled or disable (uncheck) it and assign the proper IP Address and Net Mask for your WAN port. If your connection to the Internet is through the WAN port, follow the onscreen instructions: select **WAN** in the **Gateway Parameters** group, then enter a **Host Name** in the field provided.


Firewall - IP Wizard Setup
IP Ports Setup
WAN Port : When "ISP Assigns Dynamic IP Address and Mask" is enabled (checked) the ISP will dynamically assign the IP Address and Net Mask addresses. If your ISP does not support dynamic addressing, click "ISP Assigns Dynamic IP Address and Mask" to disable (uncheck) it, and assign the proper IP Address and Net Mask for your WAN port.
Select Port
Secured LAN
Internet LAN
WAN
ISP Assigned Dynamic IP Address & Mask
IP Address
0.0.0.0
Mask
255.255.255.0
Gateway Parameters
WAN
Internet LAN
IP Address
DHCP Assigned
Host Name
Select WAN if your connection to the Internet is provided through a DCE device connected to the WAN port. Select Internet LAN if your connection to the Internet is provided through the Internet (public) LAN port. If the Internet LAN is configured as a DHCP Client, then the IP Address will be dynamically assigned by the ISP. If the DHCP Client Option is disabled, then you must enter a valid IP Address in the IP Address field. The Host Name is a unique name given to your Firewall (contact your ISP for proper name, if required)
OK
Cancel

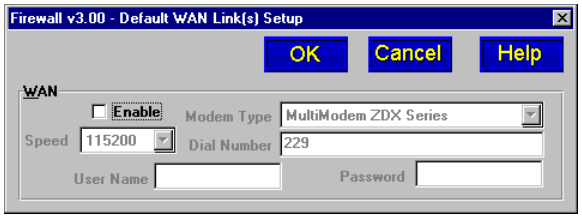
13. Click **OK** when you are finished configuring the IP parameters. The **Default WAN Link(s) Setup** dialog box is displayed.

Default WAN Link Configuration

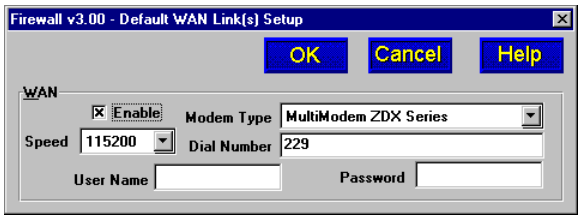
The **Default WAN Link(s) Setup** dialog box is used only if a device is connected to the **RS232/V.35** connector on the back panel of the Firewall. This connection enables your Secure (private) LAN to be connected to a local ISP for Internet service.

However, if you are using the **ETHERNET 2** port, then you will have to *disable* the RS-232/V.35 WAN port on this dialog box.

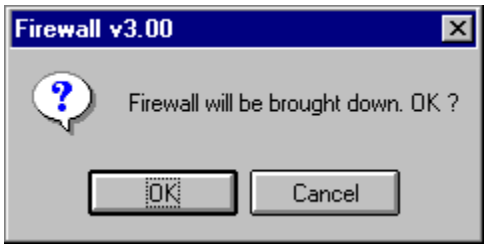
14. If a cable modem, DSL modem, or Internet LAN is connected to **ETHERNET 2**, this dialog box will appear as follows (with nothing active), click **OK** and proceed to step 19 to download the default setup to the Firewall.



If a device is connected to the RS232/V.35 connector on the back of the Firewall and you selected WAN as your Gateway on the **IP Wizard Setup** dialog box, the **Default WAN Link(s) Setup** dialog box will appear as follows, with the Enable checked and everything active; proceed to step 15 to complete the information needed on the dialog box.

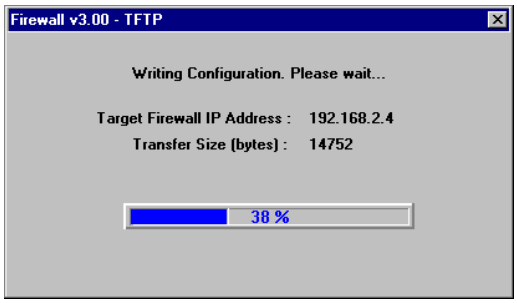


15. Click the down arrow for **Modem Type** and select from the listing the type of device that is connected to the RS232/V.35 connector, then click the down arrow for **Speed** and, if necessary, reduce the setting to the maximum speed of the connected device.
16. Click the **Dial Number** field and enter the phone number supplied by your ISP. The number can be a standard local number or it can include a long distance prefix.
17. Click the **User Name** field and enter the user name you negotiated with your ISP. The User Name can be up to 40 alphanumeric characters and is usually *not* case sensitive.
18. Click **Password** and enter the password you negotiated with your ISP. The password can be up to 15 alphanumeric characters and also is usually *not* case sensitive. Click **OK** to proceed.
19. The following dialog box is displayed.



Click **OK** to proceed.

20. The following dialog box is displayed as the setup configuration is written to the Firewall.


Firewall v3.00 - TFTP
Writing Configuration. Please wait...
Target Firewall IP Address : 192.168.2.4
Transfer Size (bytes) : 14752
38 %

21. Check to ensure that the **Fail** LED on the Firewall is Off after the download is complete and the Firewall is rebooted. This may take a couple minutes to go Off.
22. You are returned to the Multi-Tech Installation CD screen where you can now install (on your PC's hard drive) either Acrobat Reader (by clicking the **Acrobat Reader** icon) or the User Guide.

    To install the User Guide, click the **Install Manuals** icon and the file will install at **C:\Program Files\Multi-Tech Systems, Inc.\PSR1-120\Documentation** unless you browse and select an alternate directory for installation.

23. At this time your Firewall is operational. Now verify that each client PC has an IP stack loaded, workstation IP address assigned, gateway pointed to the Firewall, and the DNS name(s) supplied by ISP are entered. Refer to Chapter 5, Client Setup.

ProxyServer
Internet Access / Firewall

Chapter 4 - Firewall Software

MultiTech® Systems

Introduction

This chapter describes the operating software used in the Firewall and explains how to make changes to the configuration of your Firewall. The major configuration parameters were established during the loading of the software (Chapter 3). The Firewall software and configuration utilities allow you to make changes to that initial configuration.

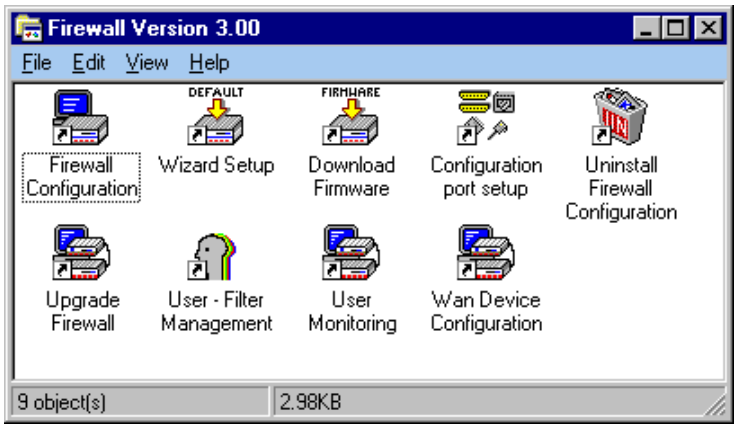
The basis of the Firewall software is a main menu (**Firewall Setup**) that enables you to consider all the parameters for a particular feature (e.g., Internet access, DHCP Server addressing, and Virtual Server mappings). These features, along with others are discussed in detail in the Firewall Configuration section later in this chapter. The other eight configuration utilities offer additional functionality.

Wizard Setup guides you through the initial configuration and software downloading, as described in Chapter 3. **Download Firmware** enables you to manually download a new version of firmware (a binary file, fwxxx.bin) from your PC's hard drive to the Firewall. The **Configuration Port Setup** utility enables you to change the method by which your PC accesses the Firewall (i.e., direct connection to the Command Port on the Firewall, or via your Internet connection to the LAN port on the Firewall). **Uninstall Firewall Configuration** removes the Firewall configuration software from your PC. The **Upgrade Firewall** feature checks the Firewall, downloads the default setup, then downloads two binary files (newboot.bin and fwxxx.bin) that upgrade the Firewall. **User - Filter Management** enables you to establish a User Database, add Groups and Users to the database, and assign authentications to the Groups, and the **User Monitoring** feature enables you to display a **User Log** dialog box where you can monitor the current history of any available server and scroll through a given day's user activity. The **WAN Device Configuration** utility enables you to configure the WAN port.

Your Firewall software includes a context-sensitive Help system. Clicking the Help button on any given dialog box provides definitions and recommended values for each button, option, and field for that dialog box. In some instances, you will also see a list of related topics that can be displayed by clicking green, underlined text. In addition, you can use the Index tab to search for definitions and references to specific terms, fields, and recommended values where applicable.

Before You Begin

The Firewall software operates in a Microsoft Windows environment. The **Firewall Version 3.00** program group, with all the utilities described above, is accessible by clicking **Start | Programs | Firewall Version 3.00 | *(utility)***, or by double-clicking the applicable shortcut icon in the program group in **My Computer** (i.e., **C:\Windows\Start Menu\Programs\Firewall Version 3.00** in Windows 95/98/NT). The program group is shown here:



Firewall Setup

All changes to your Firewall configuration are initiated through the **Firewall Setup** menu. To view or change your Firewall's configuration, click the **Start** | **Programs** | **Firewall Version 3.00** | **Firewall Configuration**. After loading, the **Firewall v3.00 - Setup** menu will appear. You can also start Firewall configuration from **My Computer** by double-clicking the **Firewall.300** folder on your local drive, then double-clicking the **Roucon** (or **Roucon.exe**) file icon. After loading, the **Firewall Setup** menu will appear.

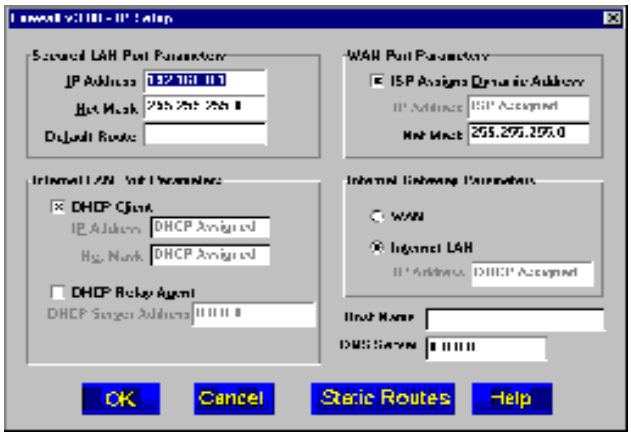
The **Firewall Setup** menu consists of 13 buttons, eleven of which enable you to display and change the IP settings, define the WAN ports, change features such as the Internet, DHCP Server, Proxy Server, and Virtual Servers, display statistics on the WAN port, control activation of Telnet, TFTP, and Web servers and dumb terminal management, test the communications link, print messages received from the target Firewall, and download setup information to the Firewall.

In addition to the **Statistics** button, two other buttons on the bottom row enable you to open the on-line Help system (Firewall Setup Help) and end (Exit) a Firewall configuration session.

Note: Pressing the **Built-In Test** button displays the **Diagnostics** dialog box which enables you to perform certain hardware tests on the WAN and LAN links. The **Print Console** option brings up the console terminal that displays any print messages received from the Firewall.

Changing IP Parameters

The **IP Setup** dialog box displays the IP addressing for your private LAN, Public LAN, and (if the Firewall is connected directly to the Internet) the WAN port. To change the IP Setup parameters that were configured during the initial setup, click **IP** on the **Firewall Setup** menu. The **IP Setup** dialog is displayed.



The **Secured LAN Port Parameters** group is used to assign the Ethernet parameters of your private LAN (connected to the ETHERNET 1) port. If a router is used to connect a second private LAN, the IP address of that router is also entered in this group.

IP Address - This field defines the IP address of the private LAN port (ETHERNET 1) on the Firewall. This must be a unique host IP address that falls within the LAN IP network, and can be an unregistered address.

Net Mask - This field defines the Subnetwork Mask of the private LAN port (ETHERNET 1) on the back panel of the Firewall.

Default Route - This field defines the IP address of a router on the private LAN that connects a second private LAN to the Firewall.

The **Internet LAN Port Parameters** group is used to configure the public LAN port (ETHERNET 2). The parameters of this group will vary, depending on the LAN configuration. The Internet LAN Port Parameters group defines the static or dynamic addressing scheme for the public LAN (connected to ETHERNET 2 on the back panel of the Firewall).

DHCP Client - The DHCP (Dynamic Host Configuration Protocol) Client option can be used if your Internet Services Provider (ISP) is able to dynamically provide the registered Internet IP addresses. However, if your ISP uses static IP addressing, the DHCP Client option must be deactivated and the IP Address field becomes active. The static IP address is then entered in this field.

IP Address - If the DHCP Client option is active, this address is dynamically assigned by the ISP. If the DHCP Client is inactive, then the static IP address of the router connected to the Internet Services Network is entered in this field.

Net Mask - If the DHCP Client option is active, the Net Mask is dynamically assigned by the ISP. If the DHCP Client is inactive, then the Net Mask provided by the ISP for the Public LAN is entered in this field.

DHCP Relay Agent - This option enables the Firewall to relay IP address requests from the Internet through the WAN to the DHCP server. If this option is enabled, the **DHCP Server Address** field becomes active, awaiting entry of the IP address of the DHCP server.

DHCP Server Address - If the DHCP Relay Agent option is active, enter the IP address of the DHCP server in this field.

The **WAN Port Parameters** group is used to configure the WAN port, if enabled. The WAN port parameters are established when the Firewall is directly connected to the Internet via the RS232/V.35 connector on the back of the unit.

ISP Assigns Dynamic Address - Normally, the ISP assigns a dynamic address when the port comes up. If this is not the case, disable this option and assign a valid registered Internet address in the IP Address field.

IP Address - If dynamic addressing is enabled, this address is dynamically assigned by the ISP. However, if static addressing is enabled, enter a valid Internet address in this field.

Net Mask - Enter the Subnetwork Mask for the WAN port in this field.

The **Internet Gateway Parameters** group is used to configure the Internet gateway if used by the Internet LAN (connected to the ETHERNET 2) port.

WAN - If a connection to the Internet Services Network is provided via a DCE device connected to the RS232/V.35 port on the back of the Firewall, then this option must be selected.

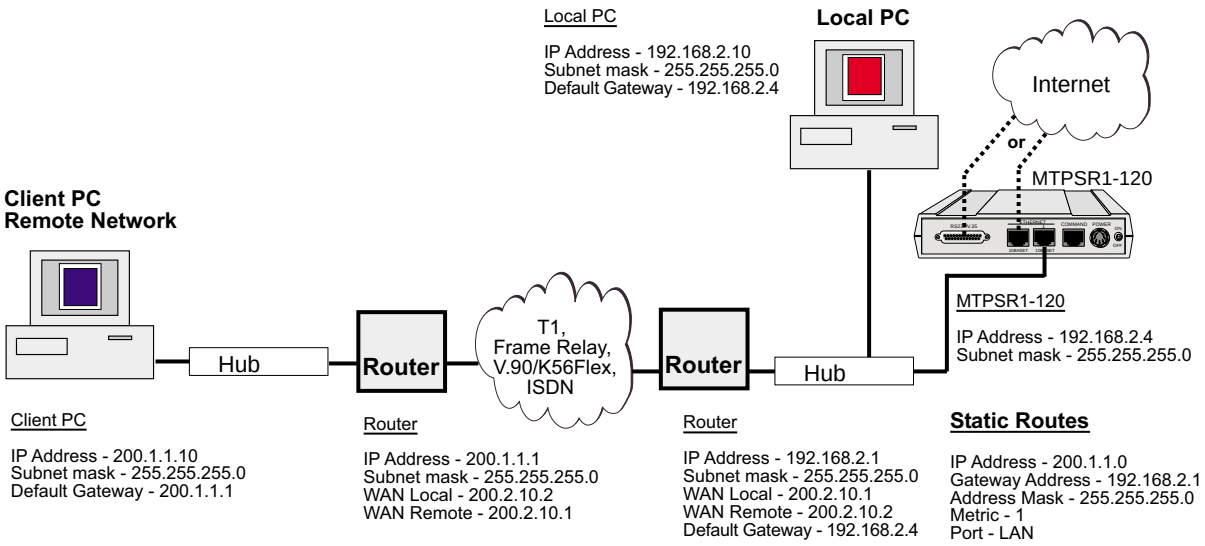
Internet LAN - If the Internet Services Network is connected to ETHERNET 2 on the back panel of the Firewall, then this option must be selected.

IP Address - If the Internet LAN is configured as a DHCP Client, this address will be dynamically assigned by the ISP. However, if the DHCP Client option is disabled, the IP Address of the device (DSL, router, etc.) must be entered in the IP Address field.

Host Name - Some cable modem providers require that a Host name be authenticated before the link will go up; therefore, if your connection to the Internet is through the WAN port and an external cable modem, you should enter the Host Name (if any) you received from your service provider.

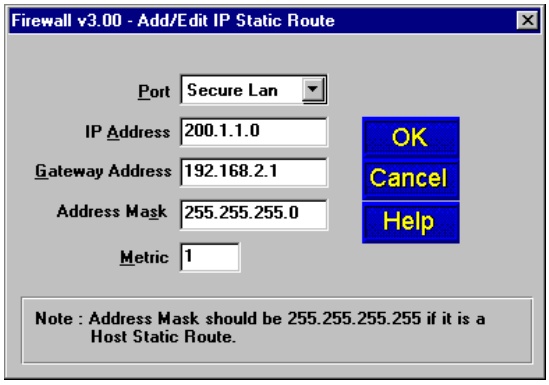
DNS Server - This field identifies the IP address of the domain name server responsible for resolving domain names for the client systems. If you use the Internet LAN port and DHCP is enabled, leave the default 0.0.0.0 and the DHCP Server will supply the IP address; however, if you use the WAN port you will need to enter the DNS Server's IP address.

The **Static Routes** feature enables a remote client PC to access the Internet through a predefined route (the static route). Static routing is used when a part of an internetwork can only be reached by one particular path. Static routes are manually configured routes that specify the transmission path a data packet must follow based on the data packet's destination address. In the example below, a data packet sent from the remote client PC to access the remote Internet through the MTPSR1-120 must have IP Address 200.1.1.0 and Gateway Address 192.168.2.1 (entered as the Static Route configuration). This determines the return path the data packet will take back to the client PC.



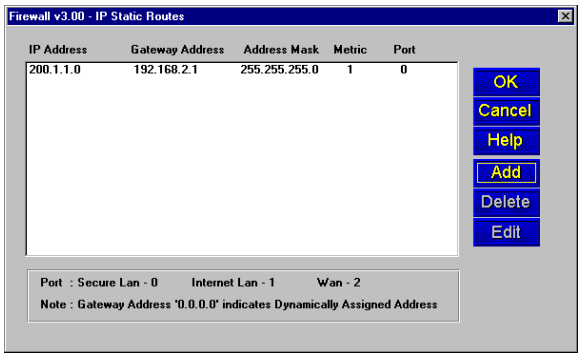
Note: You can edit or delete static routes by clicking the **Edit** or **Delete** buttons.

When the **Add/Edit IP Static Route** dialog box is displayed, select and key in the appropriate information for setting up the static route.



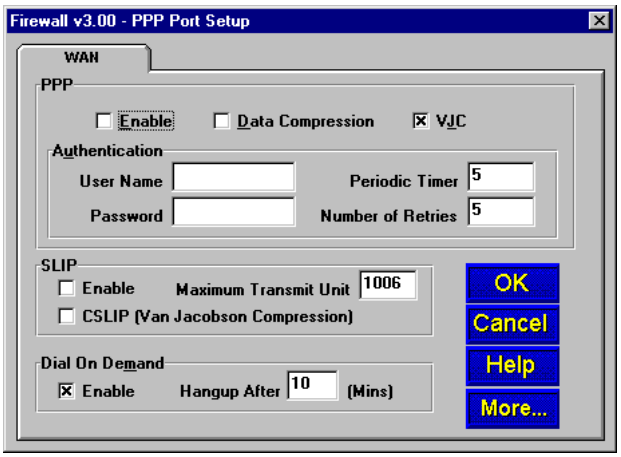
Port is the type of port, usually LAN. The **IP Address** must be the address of the target host or network in the static route (In our example, Static Route IP Address 200.1.1.0 indicates that PC clients on Routers with IP addresses beginning with 200.1.1 will be included on the static route). The **Gateway Address** must be the IP address of the local router (Gateway Address 192.168.2.1) on the next hop toward the target host and the port (i.e., LAN) with which it is associated. The **Address Mask** is the IP subnetwork mask (255.255.255.0) of the target host, and the **Metric** is the hop count (1) to the target host.

Once you have entered all the necessary information, click **OK**. The static route is displayed in the window on the **IP Static Routes** dialog box.



Changing PPP/SLIP Parameters

The Point-to-Point Protocol (**PPP**) **Port Setup** dialog box will have the PPP group activated if you decided during your initial configuration that your secure Internet connection would be through a DCE device connected to the WAN port on the Firewall and you entered a user name and password on the **Default Wan Link(s) Setup** dialog box.



Of the two protocols (PPP and SLIP), the PPP Protocol is the more robust: it allows the endpoints to "negotiate" the use of the link and protocol parameters in a standardized way and provides for standardized encapsulation of the packets. SLIP is an older protocol which requires manual authentication using a script.

If PPP is enabled, then by default the **VJC** (Van Jacobson Compression, a header compression) option is also enabled. Verify with your ISP to ensure that they support VJC.

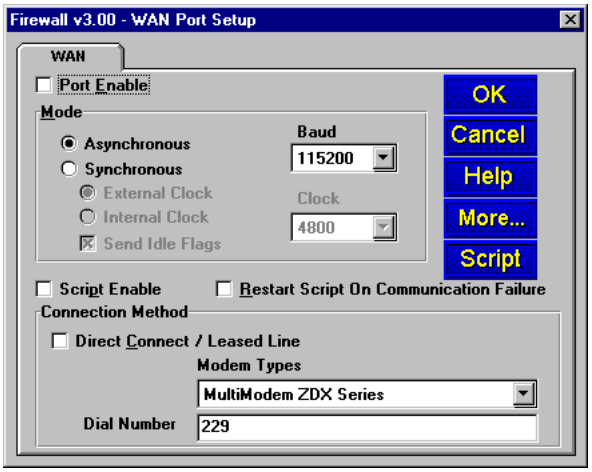
The **Data Compression** option on this dialog box compresses the entire data packet. DO NOT ENABLE this option if you are downloading (from the Internet) data that is already compressed; the extra attempt to compress the packet data will probably greatly slow down the download process.

If your ISP supports SLIP (Serial Line Internet Protocol), you will have to inactivate the PPP Enable option and activate the SLIP Enable option. If the ISP supports TCP/IP header compression using VJC, then you should also enable the CSLIP option.

If an *asynchronous* DCE device is connected to the WAN port and you want to take down the connection during idle time, you can enable **Dial On Demand** and then set your **Hangup After** option to drop the line after several minutes. The Firewall will automatically bring up the line again the next time data is available. **Note:** Dial On Demand is *not* supported if a Direct Connect Method is selected on the **WAN Port Setup** dialog box.

Changing WAN Port Parameters

The **WAN Port Setup** dialog box will display WAN port parameters if you decided during your initial configuration that your secure Internet connection would be through a DCE device connected to the WAN port on the Firewall. If your Internet connection is via a LAN connection, then the **WAN Port Setup** dialog box is inactive.



If you decided in the IP Wizard that your Private Internet LAN connection is going to be through a DCE device connected to the RS232/V.35 port on the Firewall, then the **WAN Port Setup** dialog box will appear with the **Port Enable** feature active, if an Asynchronous modem was selected in the **Default WAN Link(s) Setup** dialog box in the Wizard, that modem would be displayed in the **Modems Type** window of the **Connection Method** group, and the ISP phone number that you entered in the **Dial Number** window of the **Default WAN Link(s) Setup** dialog box will appear in the **Dial Number** window of the **Connection Method** group.

If the DCE device connected to the RS232/V.35 port on the Firewall is a synchronous device, then the Mode group on this dialog box has to be changed to Synchronous and the clocking of the device determined. If the DCE device provides the clocking, then the **External Clock** option needs to be enabled. If the clocking is provided by the Firewall, then **Internal Clock** option needs to be enabled. If the DCE device requires sending flags during idle, then the Send Idle Flags option needs to be enabled in the Mode group. If Internal clocking is enabled, then the Clock window needs to be changed to the clock speed of the synchronous DCE device which ranges from 4800 bps to 2.048 Mbps.

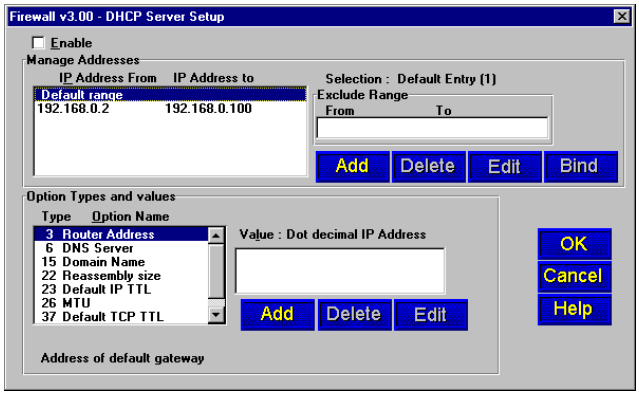
If an asynchronous device is being used as the DCE device and the ISP requires a script, then the **Script Enable** option should be activated. To compile, edit, or download a script, click the Script button. If you also want to **Restart Script on Communication Failure**, then activate that option. Script commands and a typical example of a script are provided in Appendix C.

Enabling the DHCP Server

The Multi-Tech Dynamic Host Configuration Protocol (DHCP) Server feature of the Firewall manages all the IP address assignments on the local/private LAN; thus, IP address management becomes completely transparent. The DHCP Server maintains a list of available IP addresses, and when a client computer asks for an address, the DHCP Server sends the IP Address to the client. The client computer is then able to participate in the TCP/IP network.

What are the advantages of DHCP? Why not let your systems administrator assign permanent IP addresses? Because DHCP assigns IP addresses only to computers that are active on a TCP/IP network; nonactive computers do not need to reserve an IP address. This helps workgroups that have a limited number of available IP addresses. DHCP also simplifies the process of setting up clients. Instead of having to remember which IP addresses you've assigned and which addresses are still available, you can simply configure the client for DHCP and let the DHCP server do the rest. (Refer to Chapter 5 - Client Setup.)

To display the **DHCP Server Setup** dialog box, click the **DHCP Server** button on the **Firewall Setup** menu. To enable the DHCP Server, click (check) the **Enable** option, then make additional choices as necessary.



The **DHCP Server Setup** menu enables you to customize each client PC configuration from one central point. The **Manage Addresses** group enables you to establish the range of IP addresses for the workgroup (From - To). You can then exclude specific addresses from that range in the **Exclude Range** field. Excluded addresses (individual IP addresses or ranges of addresses) are computers with static IP addresses (e.g., a DNS server, a WINS server, and the DHCP server itself). You can also add, delete, edit and bind addresses using the corresponding buttons in this group.

The **Option Types and Values** group at the bottom of the dialog box enables you to customize the configuration of the client platform. You can add, delete, or edit an option by highlighting it and clicking the appropriate button. You cannot, however, edit or delete entries provided in the default list.

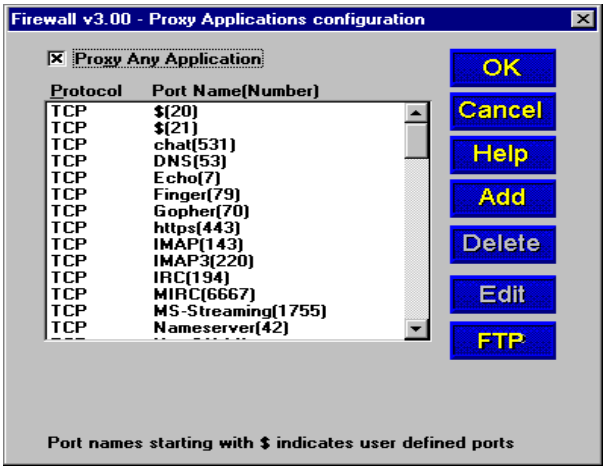
This group includes the Router Address which is the location on the IP subnet that a client can use; the Domain Name which is the human-readable Internet name of your IP domain; the Reassembly size, which sets a maximum datagram reassembly size; the Default IP TTL, which sets the IP time-to-live limit (max. 255); the MTU (Maximum Transmit Unit), which sets the largest possible unit of data that can be sent; the Default TCP TTL, which sets the TCP time-to-live limit; and the Lease time option, which sets the time duration that an IP address is assigned to a client.

When a client requests an IP address, it is given that address for a specific duration of time. When the time duration expires, the client must either receive an extension on the lease or receive another IP address to use. The default lease is 65535 seconds (18.2 hours). Assigning lease time depends on your goals and the site's usage patterns. For example, if you have more users than IP addresses, a shorter lease (hours) would be appropriate; however, for students at a university, and those in other situations where their computers are turned off for a long period of time (and you want them to keep their IP addresses), then a longer lease (weeks) would be appropriate.

Adding Proxy Applications

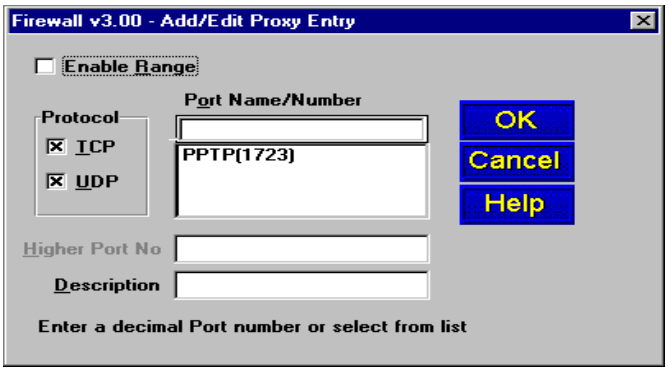
The **Proxy Applications configuration** dialog box enables the ProxyServer systems administrator to configure the set of applications available for proxying by the Firewall. This list includes many of the most common port usages; however, not all port usages are included because increasing the number of supported port usages may result in a possible decrease in performance speed and an increased security risk.

Refer to RFC 1700 on the Internet which defines the Internet Protocol suite. RFC 1700 identifies the parameters, such as Internet address, domain names, autonomous system numbers, protocol numbers, port numbers, and many others. Once the necessary information has been determined, you can add the application(s) to the supported list. Once it has this information, the Firewall will route packets through to the Internet from the unknown software.



The option to add Proxy applications is important as new software programs are continually being developed to perform useful tasks. For example, you may want to add new database managers, spreadsheets, communications packages, graphics programs etc. -- anything that would make your job easier.

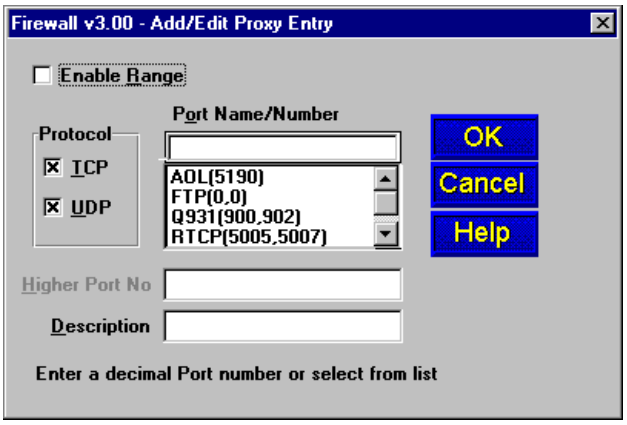
Editing considerations might involve enabling/disabling protocols individually (both TCP and UDP are enabled by default), changing the Port Name (i.e., Description) to something more easily identifiable, or changing the *range* of port numbers to exclude/include other users. (Refer to the Firewall **Helps** for details.)



Refer to RFC 1700 on the Internet which defines the Internet Protocol suite. RFC 1700 identifies the parameters, such as Internet address, domain names, autonomous system numbers, protocol numbers, port numbers, and many others. Once the necessary information has been determined, you can add the application(s) to the supported list. Once it has this information, the Firewall will route packets through to the Internet from the unknown software.

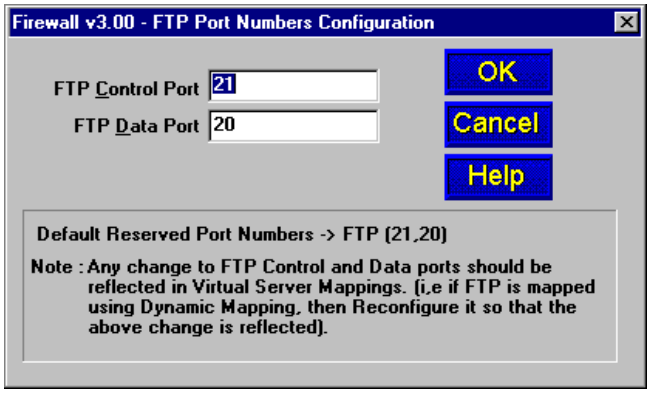
Note: Adding applications may decrease performance speed and increase security risks; therefore, you may want to delete unused or rarely used applications.

The **Add/Edit Proxy Entry** dialog box appears.



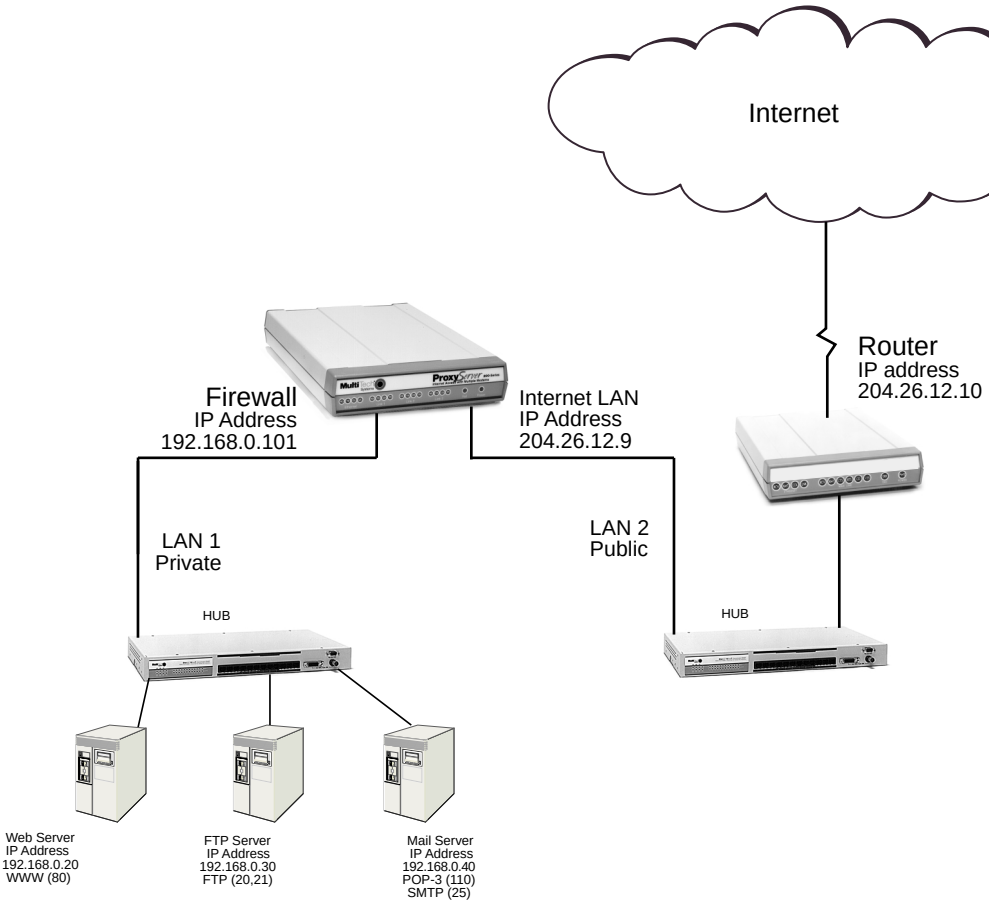
This dialog box enables you to choose the desired protocol(s) and select an existing port number from the list or enter a *new* **Port Name/Number** and **Description**. After these items are selected or entered, clicking **OK** will add the new port usage to the existing list of supported usages.

To further enhance the security of the firewall network, you can, if necessary, change the FTP Control Port and Data Port numbers from their reserved values (21 and 20, respectively, as shown below on the **FTP Port Numbers Configuration** dialog box). If you do change these numbers, be sure to notify all users who need to access the FTP server.


Firewall v3.00 - FTP Port Numbers Configuration
FTP Control Port
21
FTP Data Port
20
OK
Cancel
Help
Default Reserved Port Numbers -> FTP (21,20)
Note : Any change to FTP Control and Data ports should be reflected in Virtual Server Mappings. (i,e if FTP is mapped using Dynamic Mapping, then Reconfigure it so that the above change is reflected).

Adding Virtual Servers

The virtual server feature of the ProxyServer enables you to have multiple servers on your local area network (LAN) with one static IP address (from your ISP or Multi-Tech's Global Dynamic WAN Addressing) assigned to the WAN port (if used). A normal Internet connection requires a static IP address for each server on your LAN. A dual-LAN setup with its Internet connection through a router with its IP address assigned by an ISP is shown in the following illustration.

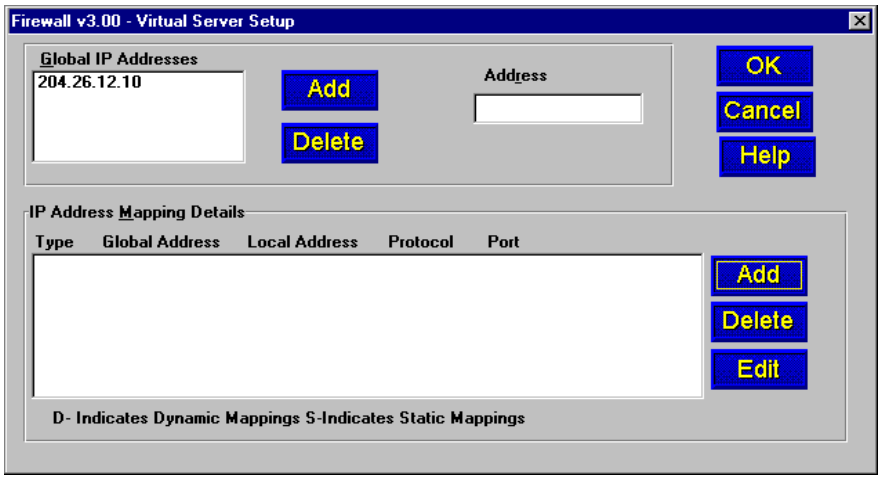


Connecting through a router to the Internet, you ordinarily need a static IP address for each function (server) you want to perform on the Internet. For example, to browse the Internet with a Web server, you need an IP address so the router knows where the traffic is coming from and where to send the reply. In our Internet connection (shown above) we have assigned an IP address of 192.168.0.20 to the Web server, address 192.168.0.30 to the FTP server, address 192.168.0.40 to the Mail (or E-Mail) server, and address 192.168.0.101 to the Firewall.

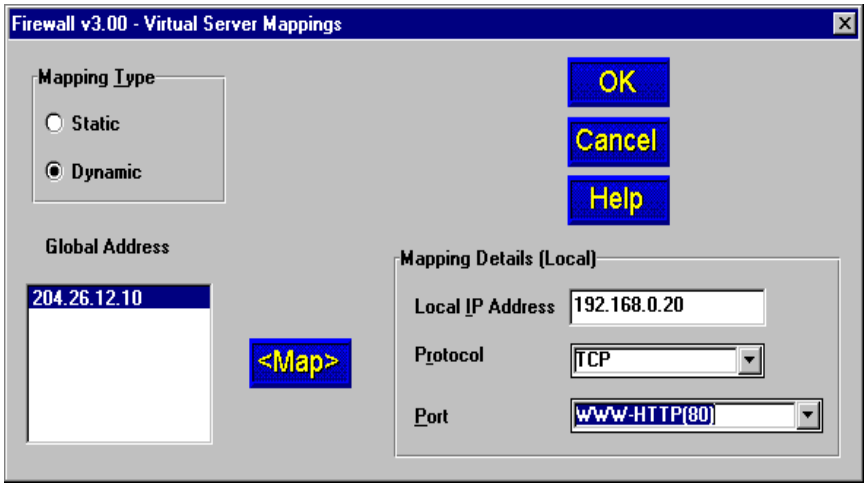
To reduce the number of static IP addresses, a virtual server feature in the Firewall enables you to map multiple local servers to a single static IP address or to a Global Dynamic WAN port address. The virtual server feature enables the Firewall to take requests from different servers (functions) and interact with the Internet based on the functionality of the request. In the normal Internet connection, this was a physical linkage to a specific IP address. However, the virtual server feature is a functional connection. Functionality is defined by how an individual server is used; i.e., the Web server uses a www-http protocol, the FTP server obviously uses FTP, and the Mail server uses the POP3 and SMTP protocols. Therefore, multiple requests can be sent to the Internet over a single physical connection and the Firewall will interpret which server is requesting service and forward all packets to the correct destination.

If instead of mapping a static IP address from your ISP, you employed Multi-Tech's Global Dynamic WAN port addressing method, you can assign a predefined Global Dynamic WAN port address to the Firewall's WAN port and then map your servers to that WAN port address the same way you map a static IP address from your ISP.

The **Virtual Server Setup** dialog box defines how the servers are connected to the one global IP address. The static IP address (of the Router) in our virtual server connection example above is added to the Global IP Addresses group in the **Virtual Server Setup** dialog box.

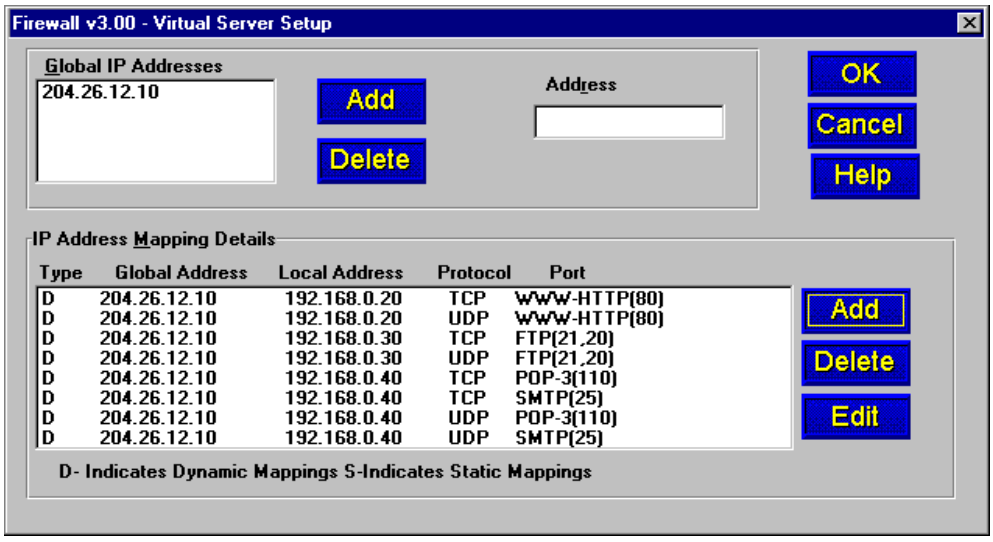


With static IP addressing, the Global IP Address is the IP address that is seen by the Internet. This global address will be used by the Firewall's virtual server feature to filter by functionality the activity of the traffic to and from the Internet. The addresses that we assigned to our servers in the virtual server example are unregistered addresses that are only seen by the Firewall. These local IP addresses are arbitrarily assigned to servers in our virtual server connection example.



These local addresses are then individually mapped (one at a time) to the global address by protocol(s) and function (or Port). The Web server, assigned the unregistered IP address of 192.168.0.20, can be mapped to the Global Address (in this case, the Router's static IP Address of 204.20.12.10) with its protocol information (TCP and UDP) and Port WWW-HTTP(80). The FTP server, with the unregistered IP address 192.168.11.30 is mapped with both TCP and UDP protocols and the port information FTP(21,20). Finally (to complete our example), the Mail server with the unregistered IP address of 192.168.0.40 is mapped with both TCP and UDP protocols and both POP-3(110) and SMTP(25) for its Port information.

After all these local mapping details are entered, they are displayed in the **IP Address Mapping Details** list on the **Virtual Server Setup** dialog box as shown on the following screen.

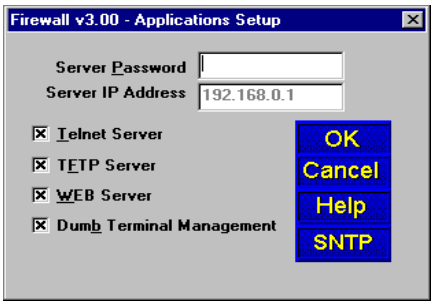


Had we accessed the Internet through the Firewall's WAN port (instead of the Router), we could've mapped the three servers on the Private LAN to a Global Dynamic WAN port address. Everything else on the Virtual Server Setup dialog box would be the same as shown on the above screen.

Managing Various Applications

In addition to local configuration, the Firewall supports various applications that enable it to be configured remotely from anywhere on the connected Internet. To manage these applications, click **Others** on the **Firewall Setup** menu.

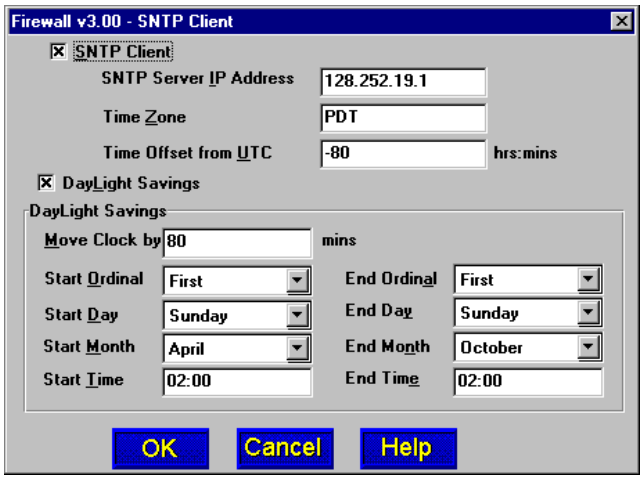
The **Applications Setup** dialog box appears (with all applications enabled, initially).



If you want to require a password to access the Firewall, define the password in the **Server Password** field; the password can be 1 to 16 characters and is *not* case sensitive. Then verify that all needed applications are enabled. To *disable* support for any of the applications (Telnet, TFTP, Web Server, or Dumb Terminal Management), click the corresponding check box to clear it.

For more information on using these remote configuration applications, refer to Chapter 5.

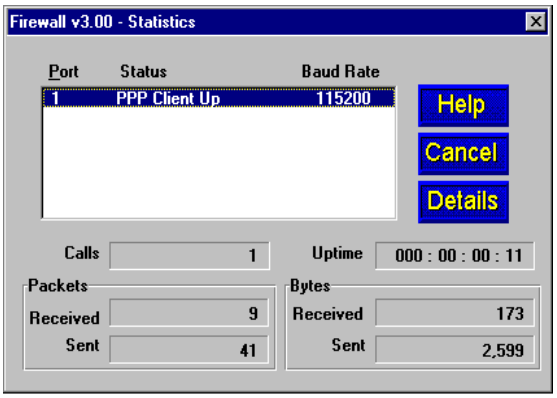
Clicking the **SNTP** (Simple Network Time Protocol) button on the **Applications Setup** dialog box displays the **SNTP Client** dialog box, where you can enable or disable SNTP Client (enabling client programs to access an SNTP server through the Firewall using the UDP protocol and port 123). The SNTP server enables you to access accurate clocks and other sources of time base information.



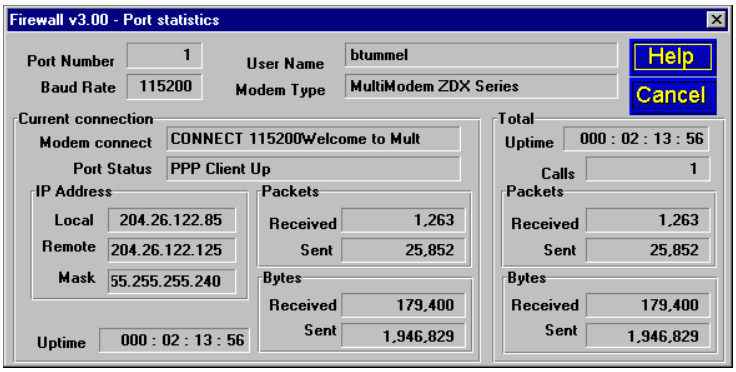
Running Statistics

The **Statistics** dialog box enables you to view the real-time WAN statistics for the Firewall. This screen shows the state of the attached external device (if any) and the current maximum baud rate.

Note: If your Internet connection is through the ETHERNET 2 port instead of the RS232/V.35 (WAN) port, you will have to use a Telnet session to gather statistics.



The read-only **Port statistics** screen (below) provides all the details relating to the traffic on the Firewall's WAN port. These statistics can be helpful in troubleshooting suspected problems at the physical layer; i.e., the WAN port itself, the link device, and any associated cabling.



All fields on this read-only screen refer to Port Number 1, which is the WAN Port. The User Name field displays the user name negotiated with the ISP for the Internet account. The maximum baud rate and modem type are also displayed.

In the Current Connection group, the Connect String field displays a message (e.g., CONNECT 115200) reported by the modem when the call connected. The Port Status field displays the current status of the selected port (e.g., PPP Client Up). The IP Address group displays the parameters of the current connection, and the Uptime field shows the amount of time that has elapsed since the current call was connected. The Packets group displays packet traffic details, and the Bytes group shows the byte-traffic details for the current call only.

Fields in the Total group at the right side of the screen show the total elapsed time since the Firewall booted up. On the screen (shown above), the uptime is 2 hours, 13 minutes, and 56 seconds. The Packets group displays the total accumulated packet traffic and the Bytes group shows the total accumulated byte-traffic for the current connection.

For additional details and parameter ranges for specific fields on the statistics dialog box, refer to the **Helps**.

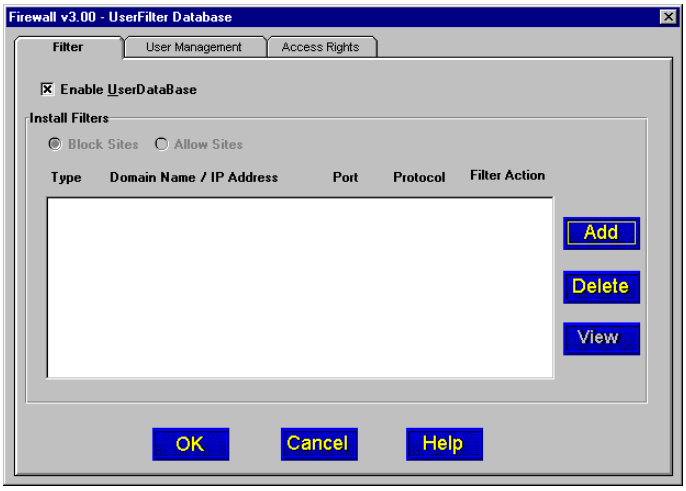
User - Filter Management

Clicking **Start | Programs | Firewall Version 3.00 | User - Filter Management** (or double-clicking the **User - Filter Management** icon on the **Firewall Version 3.00** icon group, if it is open on your desktop) displays the **UserFilter Database** dialog box with the **Filter** tab open.

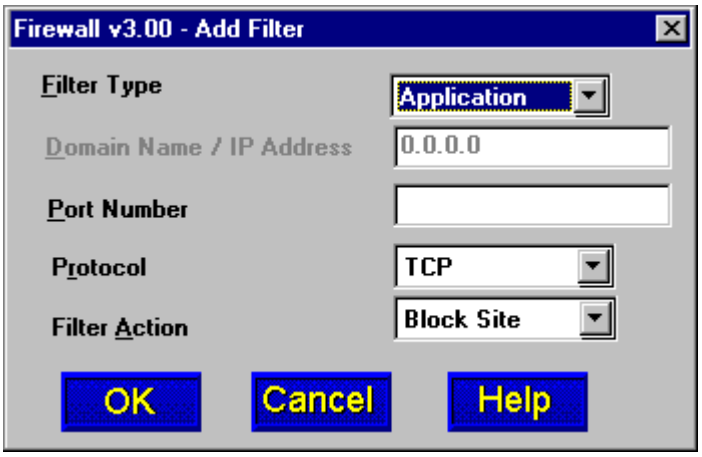
The **Filter** tab on the **UserFilter Database** dialog box displays any filters that are currently set up for the Groups using the Firewall. This feature enables the Network Administrator to selectively filter (block) or forward (allow) IP packets received by the server based on their application, domain name, IP address, or by the protocol (TCP, UDP, or TCP & UDP) and port to which they are to be sent.

In order to use *any* features on the **UserFilter Database** dialog box, you must first check (to enable) **Enable UserDataBase**. This enables the other two tabs so you can then set up Users and Groups and later manage and monitor them.

Note: If **Enable UserDataBase** is later *disabled* (unchecked), the various groups of Blocked Sites and Allowed Sites that you have set up will be applied to **everyone** on your network; i.e, there will be NO AUTHENTICATION. In normal usage, however, with **Enable UserDataBase** enabled (checked), the Web sites requiring authorization you've designated will be Blocked from certain groups you specified and the Web sites requiring authorization that you've designated to be Allowed for other groups will be available only to those specified groups.



While this tab is open, you can only add or delete filters. The **Add Filter** dialog box enables you to select the Filter Type, Filter Action (Block Site or Allow Site), and Protocol (TCP, UDP, or TCP & UDP) for a new filter to be applied to the WAN port (Port Number 1). This dialog box also enables you to *edit* an existing filter you've selected (highlighted) in the list on the **Filter** tab of the **UserFilter Database** dialog box.

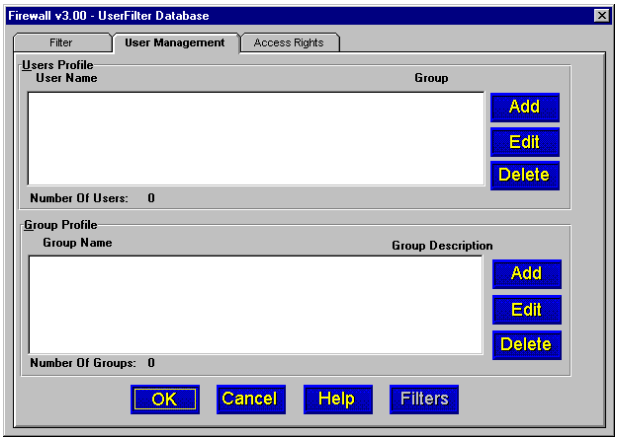


For a more detailed description of Filtering, refer to the **Helps** provided with your Firewall software.

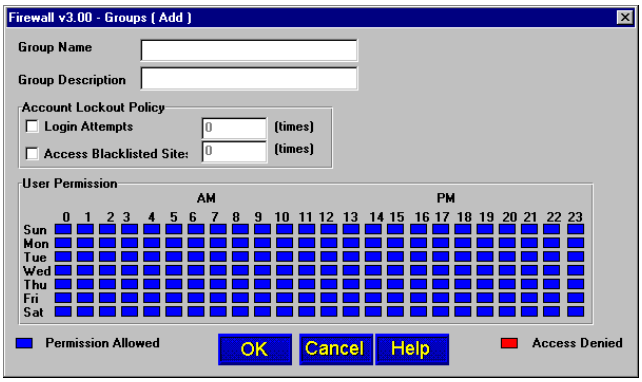
User Management

The **User Management** tab on the **UserFilter Database** dialog box enables you to add Groups and Users to the UserFilter Database. Once the User Database is enabled (checked) on the Filter tab, both the User Management and Access Rights tabs become active and can be viewed and used.

Groups are defined as administrative units comprised of one or more users with similar needs for network resources. Once users are placed in groups, resource access can be managed on a group basis rather than an individual basis. (For example, it is much easier to manage five groups of 20 each than 100 individual users.) Groups (or Workgroups) are assigned names for organizational purposes and convenience, and the group names are often descriptive, such as ENGINEERING, ACCOUNTING, or SALES.



Click the lower **Add** button to begin building your database of Groups; this will display the **Groups (Add)** dialog box, where you can assign the Group Name, Group Description, and User Permission.



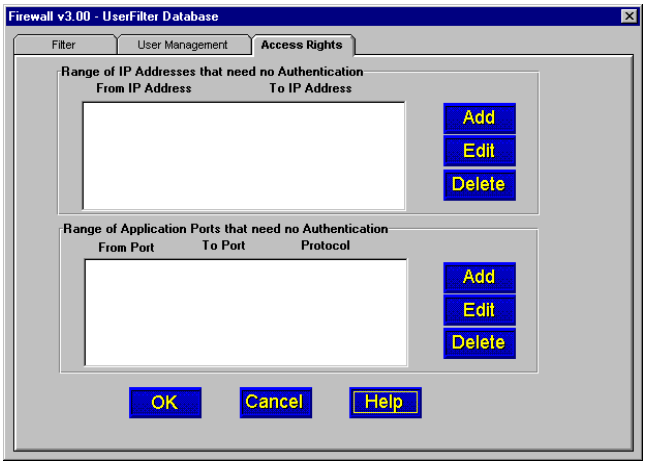
In the **User Permission** group, the permissions are based on a 24-hour clock where initially the Group is permitted access (i.e., access is *allowed*) 24 hours a day, seven days a week, indicated by the Blue color throughout. To deny Group access on any given hour(s), click those hour(s) to toggle them from blue to red (Access Denied).

This dialog box also enables you to set up an Account Lockout Policy by designating a maximum number of (unsuccessful) Login Attempts and a maximum allowable number of attempts to access a blacklisted site.

For a more detailed description of User Management, refer to the Helps provided with your Firewall software.

Access Rights

The **Access Rights** tab on the **UserFilter Database** dialog box enables you to add ranges of IP addresses where no authentication is needed; i.e., all Groups will have free access all the time. Here, too, you can add ranges of application ports (together with the corresponding protocol or protocols, TCP, UDP, or TCP & UDP) that need no authentication. Any Access Rights entries are stored and displayed in separate lists here on the **Access Rights** tab.

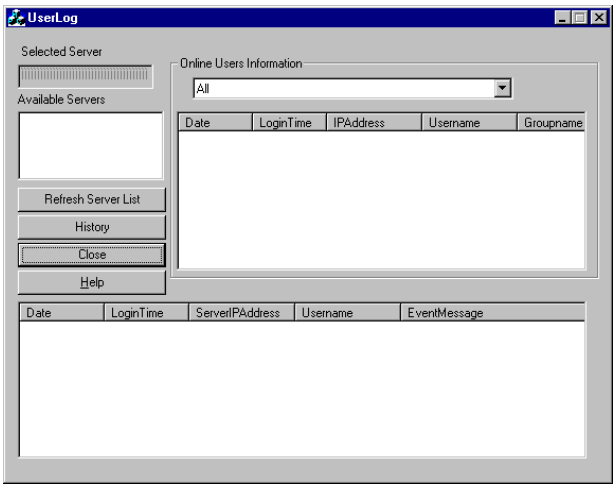


After they are added to this tab, the range entries can be edited or deleted as necessary.

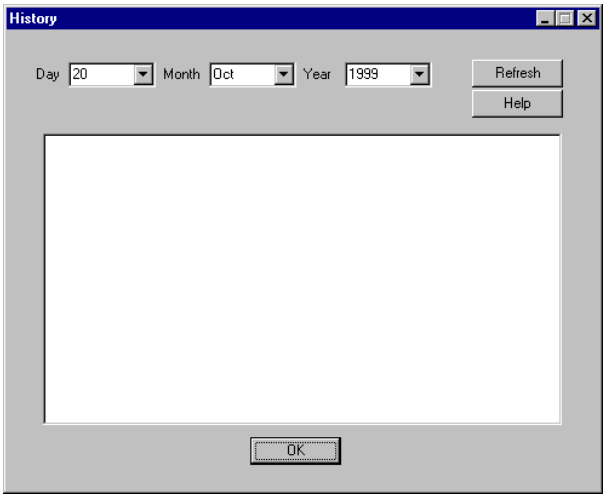
For a more detailed description of Access Rights, refer to the **Helps** provided with your Firewall software.

User Monitoring

Clicking **Start | Programs | Firewall Version 3.00 | User Monitoring** (or double-clicking the **User Monitoring** icon on the **Firewall Version 3.00** icon group, if it is open on your desktop) opens the **UserLog** dialog box. This screen displays a list of Available Servers, a Selected Server, Online Users Information (always *empty* when opened), and a growing list of any Event Messages that have occurred while this dialog box was open and/or open but minimized. **Note:** In order for this dialog box to work properly, the selected server must keep track of time in order to time-stamp the entries.



In addition to **Close** and **Help** buttons, this dialog box includes a **Refresh Server List** button and a **History** button. Clicking the **History** button displays a **History** screen (below) which enables you to view today's history or the history of events that occurred on a different day that you select.



This **History** dialog box comes up initially with today's date; however, you can use the drop-down lists for Day, Month, and Year (across the top of the dialog box) to select a different day's history of events. **Note:** If no Time Server is available/configured, you may find events are displayed only when the date is set to "**1 1 1900**."

After they are added to this tab, the range entries can be edited or deleted as necessary.

For a more detailed description of User Monitoring, refer to the **Helps** provided with your Firewall software.

ProxyServer
Internet Access / Firewall

Chapter 5 - Client Setup

MultiTech® Systems

Introduction

The information provided in this chapter enables multiple users to configure their PCs to access the Internet through a Firewall. The procedures are divided into two sections based on operating platforms. The first section covers configuration of Windows 98/95 PCs, and the second section covers configuration of Windows NT (4.0 Workstation) PCs.

Before you Begin

Before you begin the client setup process, read through the following requirements:

Firewall

The Firewall was configured by the administrator who, while installing the software, determined that the Firewall would either automatically assign Internet (IP) addresses, or require that they be assigned manually to each client PC. Also, the administrator assigned an IP address to the Firewall's Ethernet port, and assigned user names and passwords to the WAN links. All these factors play a role in client configuration. Make certain that you are aware of the decisions made prior to setting up client PCs.

PC

To access the Firewall, your PC must have communications capability including hardware such as a network card and any necessary software.

If the Firewall does not automatically assign an IP address to each PC, you will have to obtain it from your network administrator. You will also need the IP address for the Firewall (the Gateway address), and the IP Address of your organization's Domain Name Server (DNS). All these items are needed so your PC can identify the Firewall as its gateway and properly set up your network security.

Checklist

A checklist is provided toward the end of each procedure (Steps 16 and 19, respectively) so you can record all the pertinent information required for the connection between your PC and the Firewall. Keep the completed checklist as a reference for future upgrades.

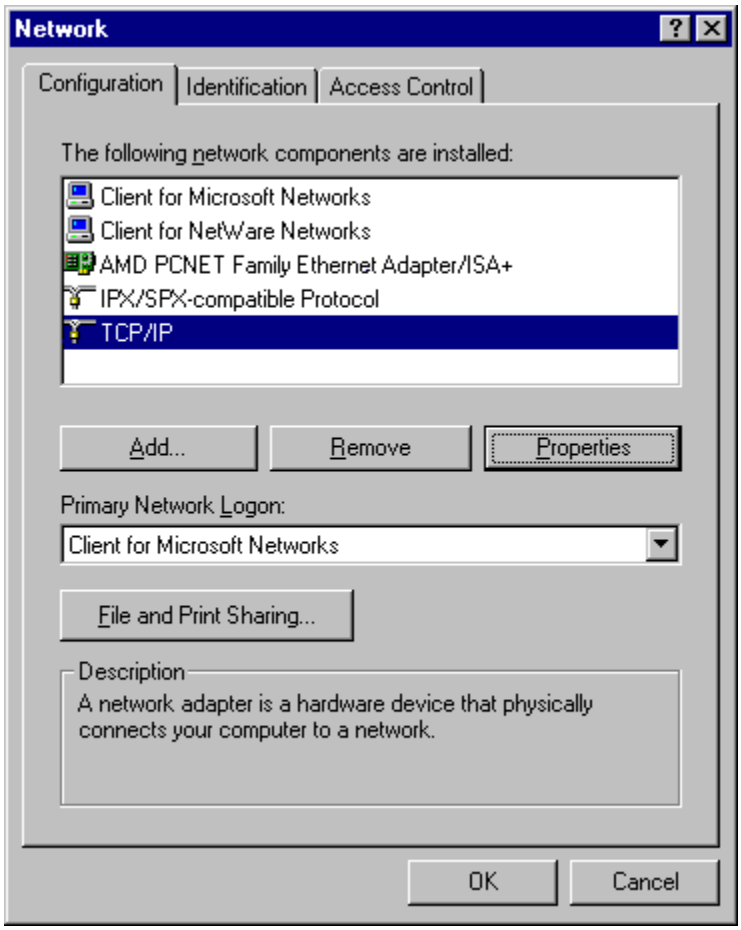
Configuring in Windows 98/95

Perform the following steps to set up your Windows 98/95 PC:

Note: All the hardware and screens used in this section are intended as examples only. Please select options appropriate to your system.

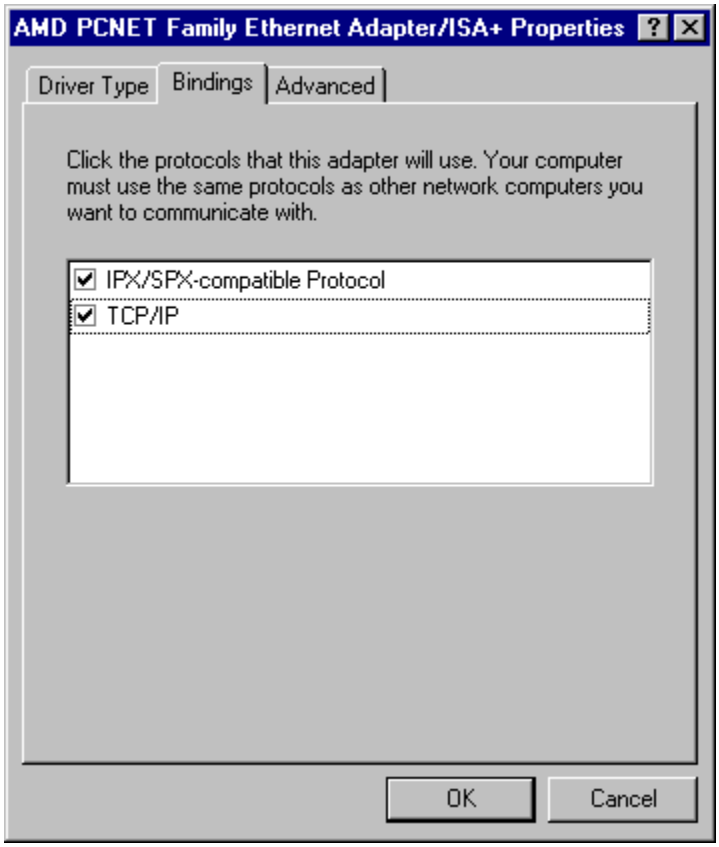
1. Click **Start | Settings | Control Panel**, then double-click the **Network** icon.

The **Network** dialog box (**Configuration** tab) is displayed which shows all the network components (e.g., clients, adapters, protocols, and any services) installed on your PC.



2. If **TCP/IP** is listed, proceed to step 3; otherwise, refer to **Installing TCP/IP (Win98/95)**, at the end of this section.

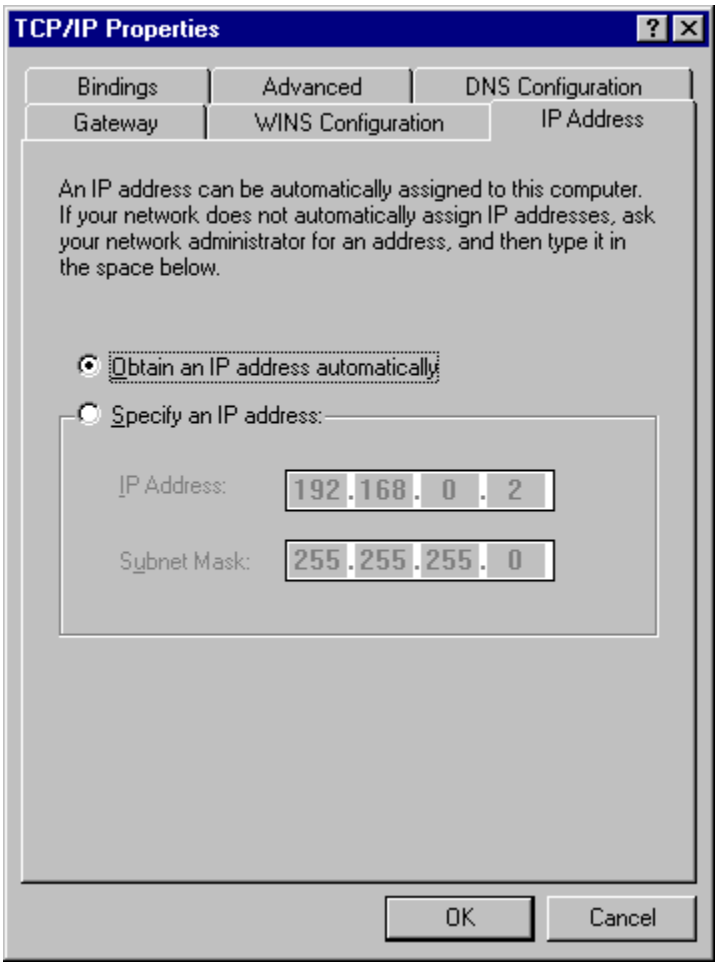
3. Check for binding between the adapter and TCP/IP. In the **Network** dialog box, click your Ethernet adapter to select it, then click **Properties** to display the Adapter Properties window.


AMD PCNET Family Ethernet Adapter/ISA+ Properties
Driver Type
Bindings
Advanced
Click the protocols that this adapter will use. Your computer must use the same protocols as other network computers you want to communicate with.
IPX/SPX-compatible Protocol
TCP/IP
OK
Cancel

4. Click the **Bindings** tab, then if necessary click the box to the left of TCP/IP so this entry is enabled (checked). When you are finished, click **OK** to return to the **Network** dialog box.

   Note: There may be other protocols listed and enabled under your Ethernet adapter. This does not affect the TCP/IP protocol. Rather, it simply means your computer will accept messages using those protocols as well as TCP/IP.

5. Select **TCP/IP**, then click **Properties** to open the **TCP/IP Properties** window.



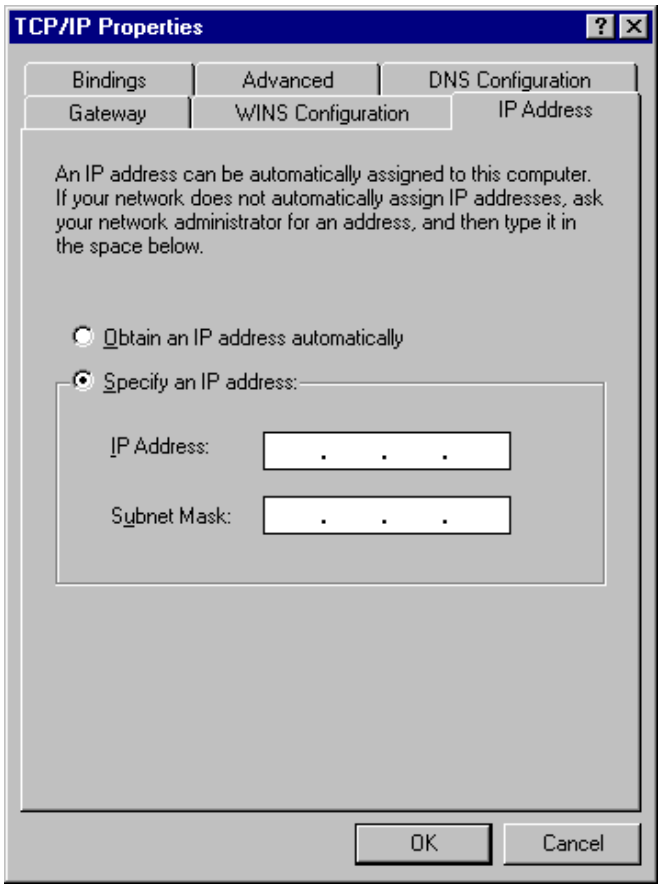
6. Select the **IP Address** tab.

   The IP addressing method depends on how your Firewall's DHCP Server option was configured. If DHCP Server is active, your IP address is issued automatically. If your network administrator did NOT activate DHCP Services on the Firewall, you will have to assign your IP address manually.

   Verify the Firewall/DHCP status with your network administrator, then proceed to step 7 for DHCP assigned addressing, or to step 8 for manual addressing.

7. If DHCP Services are active on the Firewall (default), verify that the **Obtain an IP address automatically** option is selected. You are done; go to step 17 to reboot your PC and attempt to open an Internet session.

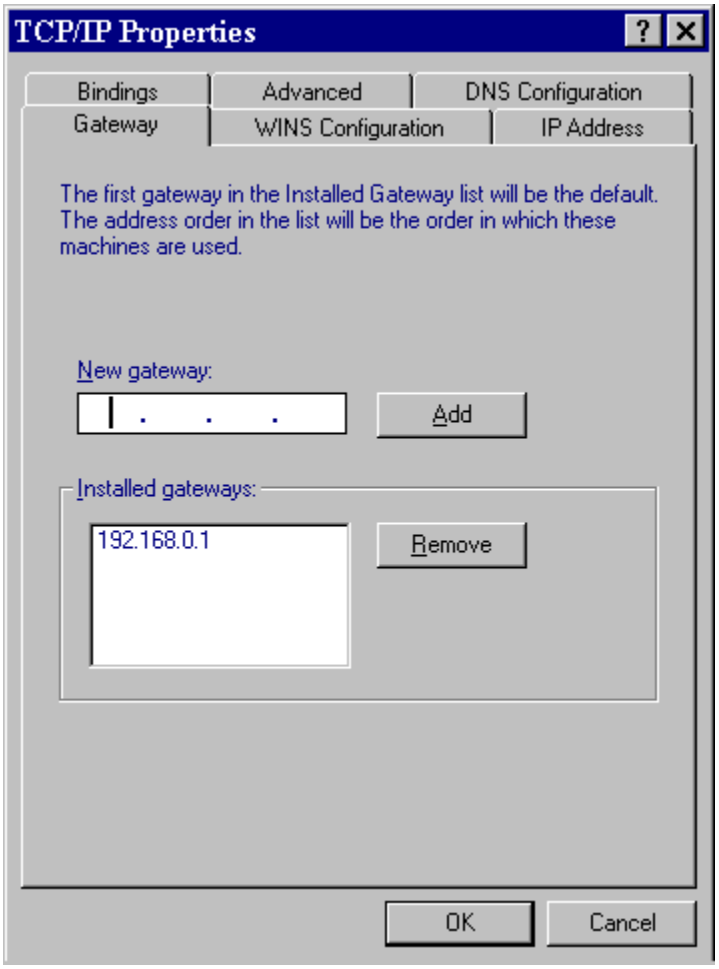
8. If DHCP Services are NOT active on the Firewall, you will have to manually enter your IP address. Select manual addressing by clicking the **Specify an IP address** option. The IP Address and Subnet Mask fields become active.


TCP/IP Properties
Bindings
Advanced
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

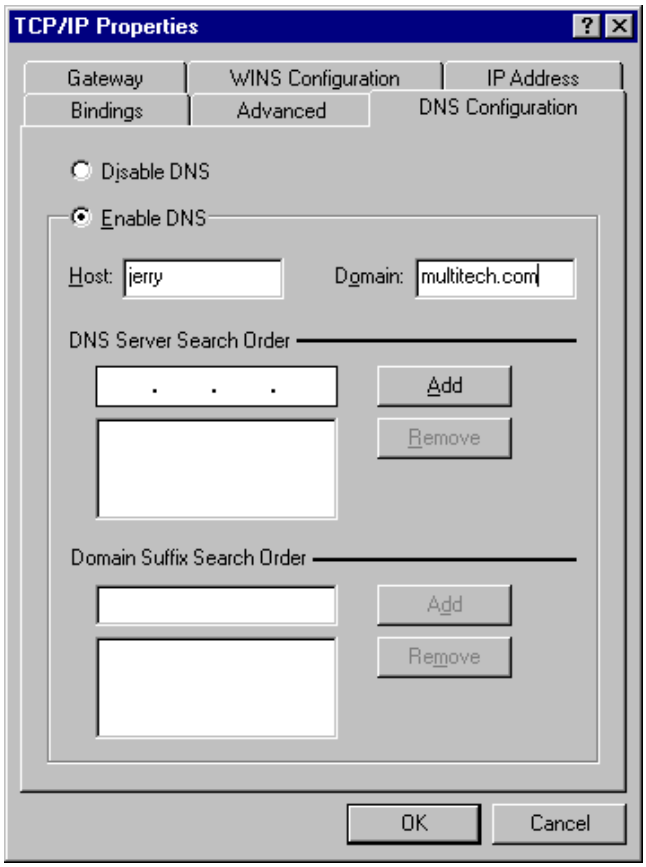
9. In the **IP Address** field, type the IP address assigned to your PC.

   Remove the default IP address (if any) and begin typing the new address. This address is entered in dotted decimal notation and is comprised of four groups (octets) separated by periods or “dots.” If a group has fewer than 3 digits, type the necessary digits and press the space bar to move to the next group. When you are finished, verify that the IP address is identical to the IP address you were given for your PC.

10. Click the **Gateway** tab.



11. In the **New gateway** field, enter the IP address of the Firewall's Ethernet port and click **Add**. The new gateway address is displayed in the list of **Installed gateways**.
12. Click the **DNS Configuration** tab. Verify that **Enable DNS** is selected (checked).



13. In the **Host** field, enter your user name (e.g., jerry).
14. In the **Domain** field, enter your company's domain name (usually the company name followed by one of the following extensions: .com, .edu, .gov, .org, .mil, or .net. For example, multitech.com).
15. In the **DNS Server Search Order** group, place the cursor in the first group of the address field and type the IP address of your LAN's DNS server (provided by your network administrator). Click **Add** and the new address is displayed in the list below the address field.

    Your network may have more than one DNS server, allowing you to use a secondary DNS server if the primary DNS server is not available. If this is the case, add the IP address of the secondary DNS server using the same procedure as with the first.

    Note: The address that is displayed first (at the top) of the list is the primary server (the first one searched). You can "drag and drop" the items in the list, if necessary, until the primary DNS server is listed first.

    When this is done, click **OK**. You are returned to the **Network** dialog.
16. In the Network dialog, Click **OK**. You are returned to the **Control Panel**.

    Use the following checklist to record all the configuration settings for future use:

Configuration Checklist	
IP Address (PC)	. . .
IP Address (ProxyServer)	. . .
Host (User Name)	
Domain	
DNS Server Address	. . .
Network Adapter (Manufacturer/Model Number)	

17. Reboot the PC for changes to take effect.

    At this point your client setup is complete. Test your setup by following steps 18 and 19. If you encounter problems, contact your administrator.

18. Initiate an Internet session by double-clicking your browser icon, or try to FTP a file.

    Note: The Firewall operates transparently, so there should not be a need for any special proxy settings on your IP applications (e.g., browser, Telnet, or FTP). Set up each application as “No Proxy” or equivalent; or, connect to the Internet over the LAN.

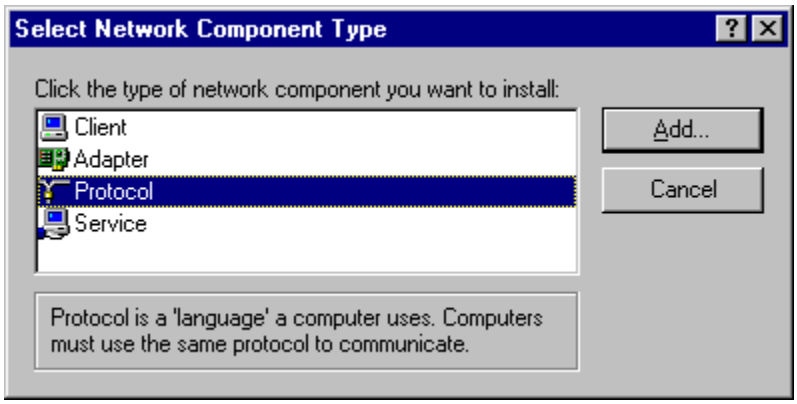
19. To further validate your connection to the Firewall, “Ping” the IP address of the Firewall.

Installing TCP/IP (Win98/95)

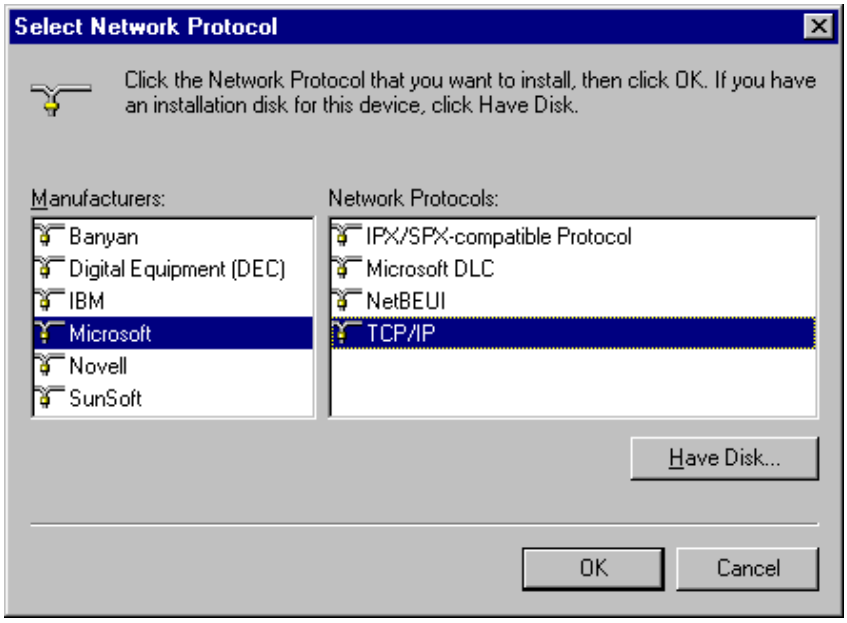
If TCP/IP is not already installed, perform the following steps:

Note: For this procedure you may need your Windows installation disks or CD ROM.

1. In the **Network** dialog box, click **Add**. The **Select Network Component Type** dialog is displayed with a list of installation options.



2. Select **Protocol** and click **Add**. The **Select Network Protocol** dialog box is displayed with protocol options.



3. In the **Manufacturers** list, click the manufacturer option (Microsoft in the example) to highlight it. A list of available protocols will appear in the **Network Protocols** list.
4. In the **Network Protocols** list, select **TCP/IP** and click **OK**.
5. Exit the add option. Click the **OK** button.

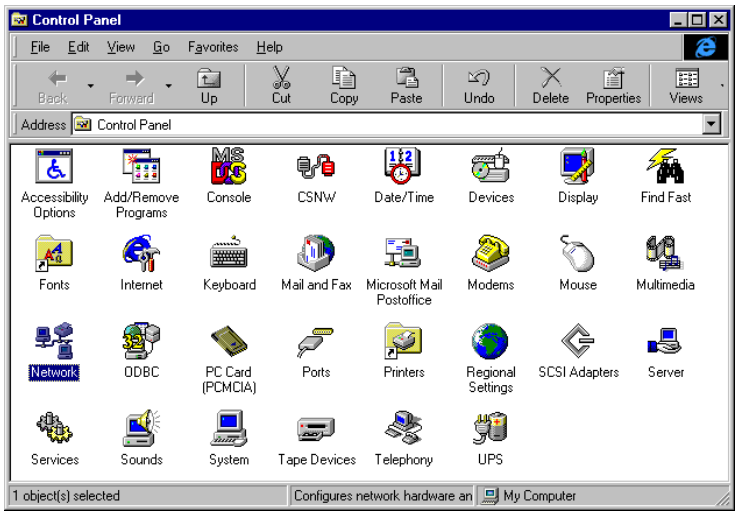
   Note: If Windows does not find the necessary files on the hard drive, click **Have Disk** and follow the onscreen instructions for loading TCP/IP from the installation disks/CD-ROM.
6. Reboot your PC for changes to take effect.
7. Click **Start | Settings | Control Panel** and double-click the **Network** icon to return to the Network dialog. Return to step 3 of the **Configuring in Windows 98/95** and continue with the client setup procedure.

Configuring in Windows NT

Perform the following steps to set up your Windows NT workstation PC:

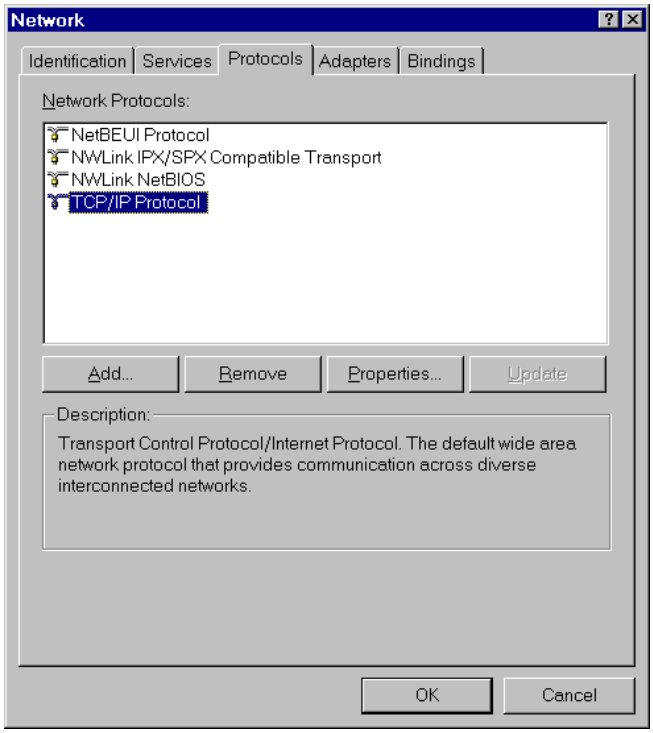
Note: All of the hardware and screen samples in this section are intended as examples only. You should select options appropriate to your network.

1. Click **Start | Settings | Control Panel.**



Double-click the **Network** icon.

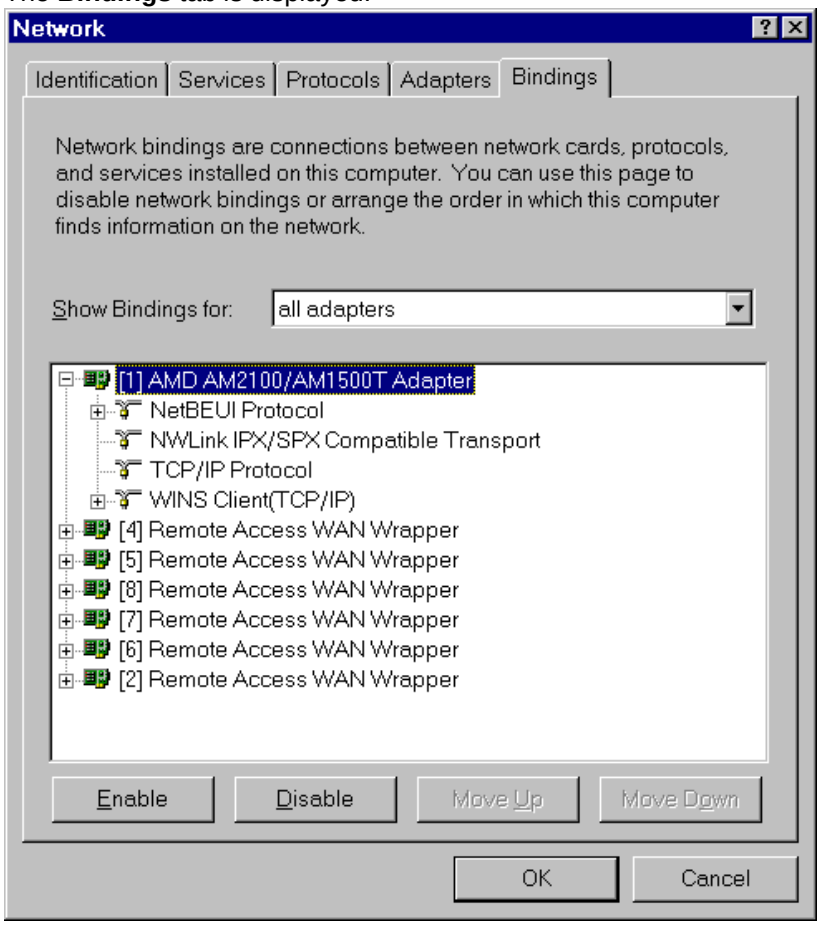
2. The **Network** dialog box is displayed. Click the **Protocols** tab.



A list of protocols currently present on your PC is displayed. Check the installed protocols. If you find **TCP/IP Protocol** listed, proceed to step 4. If TCP/IP is not listed, you must install it prior to proceeding. Refer to **Installing TCP/IP (WinNT)** at the end of this section.

Click the **Bindings** tab.

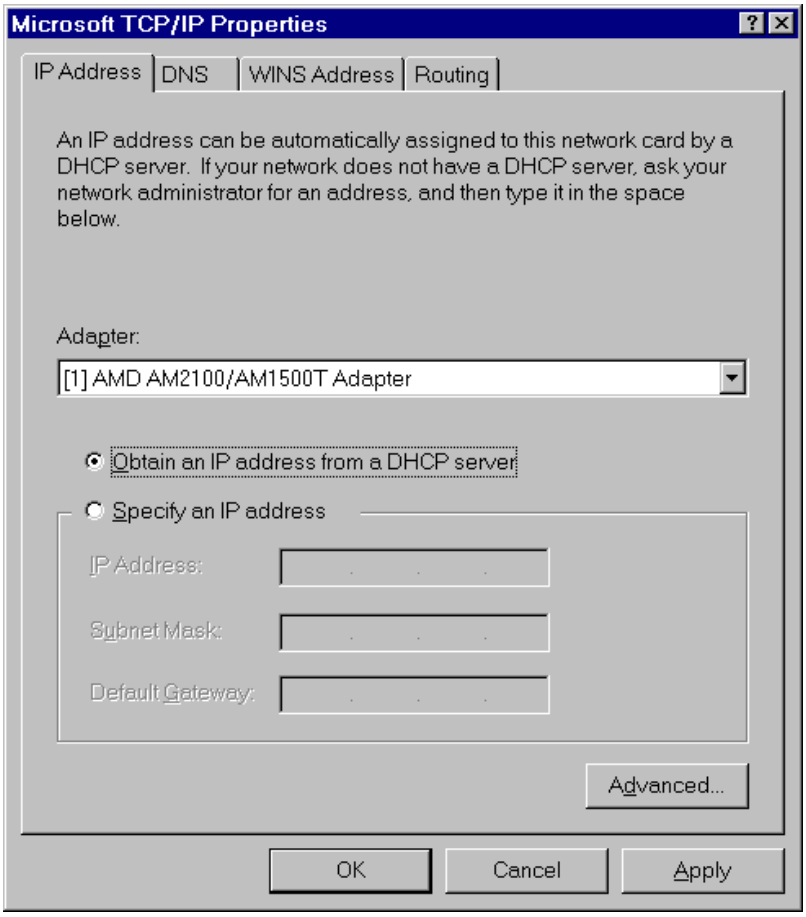
3. The **Bindings** tab is displayed.



4. In the **Show Bindings for** drop down list, select **all adapters**. A list of all adapters is displayed.
5. Double-click the entry for your Ethernet card adapter to expand the list of bindings. Verify that **TCP/IP Protocol** is included in the bindings below your adapter.

   Note: There may be other protocols in the list under your Ethernet adapter. This does not affect the TCP/IP protocol. Rather, it simply means your computer will accept messages using those protocols as well as TCP/IP.
6. Click the **Protocols** tab.

7. In the **Network Protocols** list select **TCP/IP**, then click **Properties**. The **Microsoft TCP/IP Properties** dialog is displayed.


Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
[1] AMD AM2100/AM1500T Adapter
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

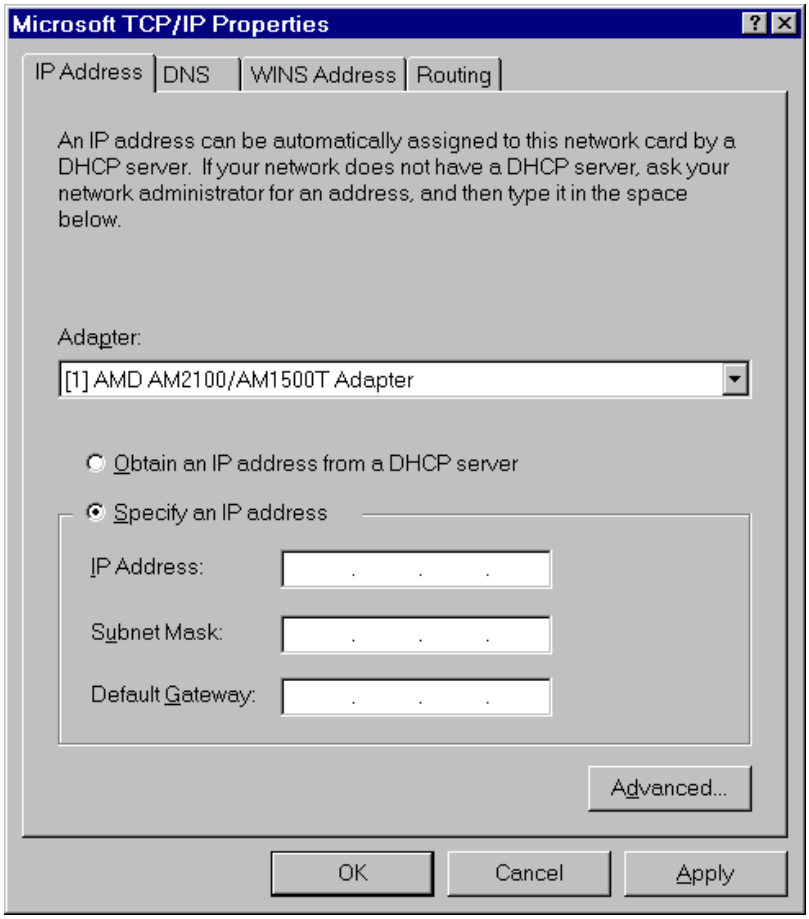
8. Click the **IP Address** tab.

   The IP addressing method depends on how your Firewall's DHCP Server option was configured. If DHCP Server is active, your IP address is issued automatically. If your network administrator did NOT activate DHCP Services on the Firewall, you will have to assign your IP address manually.

   Verify the Firewall/DHCP status with your network administrator, then proceed to step 9 for DHCP assigned addressing, or to step 10 for manual addressing.

9. If DHCP Services are active on the Firewall (the default), verify that the **Obtain an IP address from a DHCP server** option is enabled (checked). At this point, you are done. Go to step 20 and attempt to open an Internet session.

10. If DHCP Services are NOT active on the Firewall, you will have to manually enter your IP address. Select manual addressing by clicking the **Specify An IP Address** option. The IP Address and Subnet Mask fields become active.


Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
[1] AMD AM2100/AM1500T Adapter
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

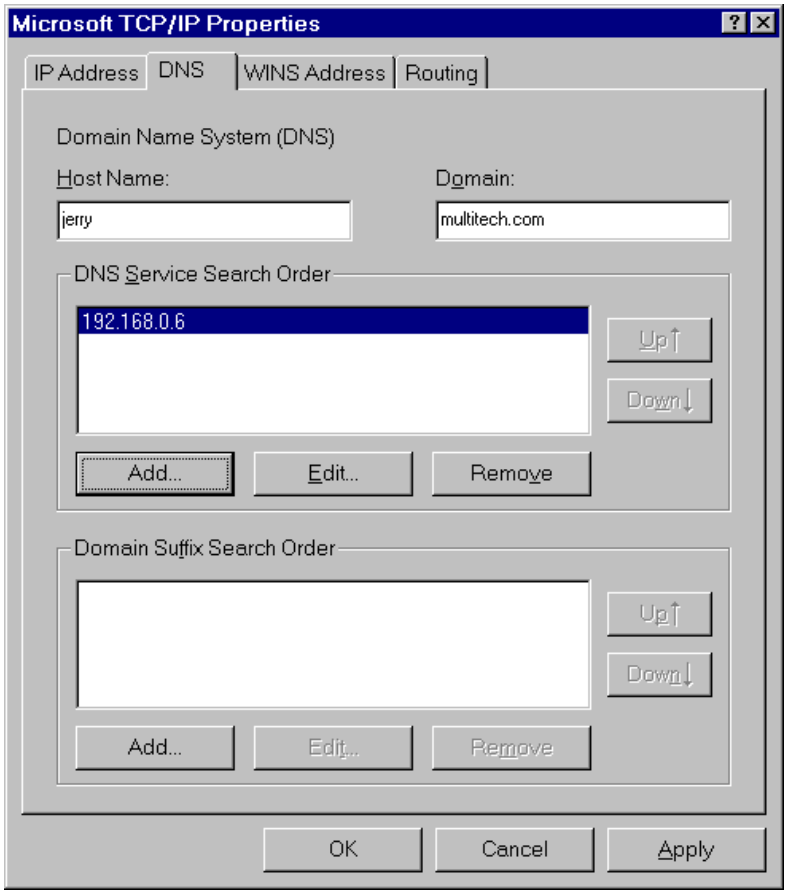
11. In the **IP Address** field, type the IP address assigned to your PC.

    Remove the default IP address (if any), and begin typing the new address. This address is entered in dotted decimal notation and is comprised of four groups (octets) separated by periods or “dots.” If a group has fewer than 3 digits, type the necessary digits and press the space bar to move to the next group. When you are finished, verify that the IP address is identical to the IP address you were given for your PC.

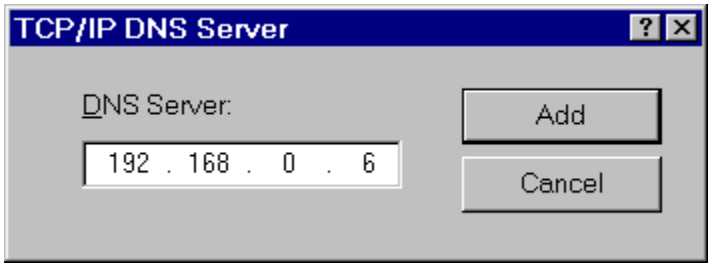
12. In the **Subnet Mask** field, type the subnetwork mask assigned by your administrator. When you are finished, verify the new mask.

13. In the Default Gateway field, type the IP address of the gateway assigned to your LAN. When you are finished, verify the new gateway.

14. Click the **DNS** tab. The **Domain Name System (DNS)** properties are displayed.



15. In the **Host Name** field, type your user name (e.g., jerry).
16. In the **Domain** field, enter your organization's domain name (usually the organization name followed by one of the following extensions: .com, .edu, .gov, .org, .mil, or .net. For example, multitech.com).
17. In the **DNS Server Search Order** group, click **Add**. The **TCP/IP DNS Server** dialog box is displayed.



18. In the **DNS Server** field, place the cursor in the first group and type the IP address of your LAN's DNS server (provided by your network administrator).

19. Click **Add**. You are returned to the **Microsoft TCP/IP Properties** dialog box, **DNS** tab, and the new address is displayed in the **DNS Search Order** list.

    Your network may have more than one DNS server, allowing you to use a secondary DNS server if the primary DNS server is not available. If this is the case, add the IP address of the secondary DNS server using the same procedure as with the first.

    Note: The address that appears first (at the top of the list) is the primary server (the first one searched). You can use the **Up** and **Down** buttons to rearrange the items in the list, if necessary, until the primary DNS server is listed first.

    When this is done, click **OK**. You are returned to the **Network** dialog box.

    Use the following checklist to record all the configuration settings for future use:

Configuration Checklist	
IP Address (PC)	. . .
IP Address (ProxyServer)	. . .
Host (User Name)	
Domain	
DNS Server Address	. . .
Network Adapter (Manufacturer/Model Number)	

20. Reboot the PC for changes to take effect.

    At this point your client setup is complete. Test your setup by performing steps 21 and 22. If you encounter problems, contact your administrator.

21. Initiate an Internet session by double-clicking your browser icon, or try to FTP a file.

    Note: The Firewall operates transparently, so there should not be a need for any special proxy settings on your IP applications (e.g., browser, Telnet, or FTP). Set up each application as “No Proxy” or equivalent; or, connect to the Internet over the LAN.

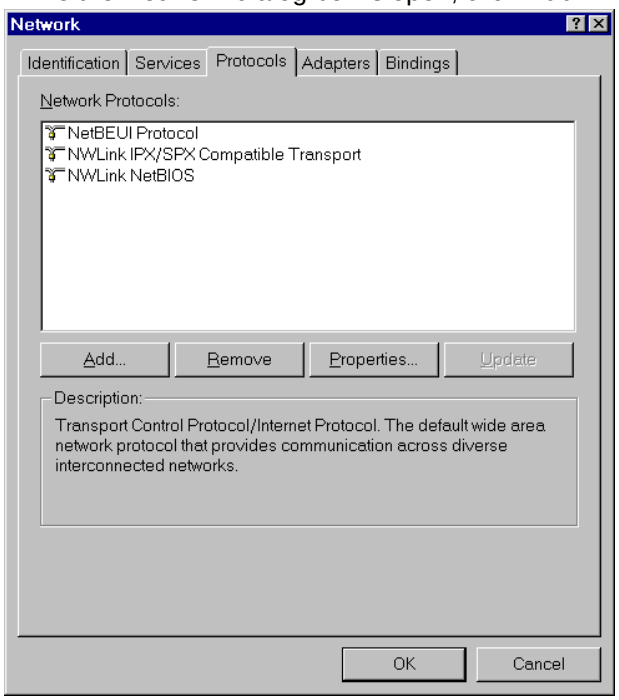
22. To further validate your connection to the Firewall, “Ping” the IP address of the Firewall.

Installing TCP/IP (WinNT)

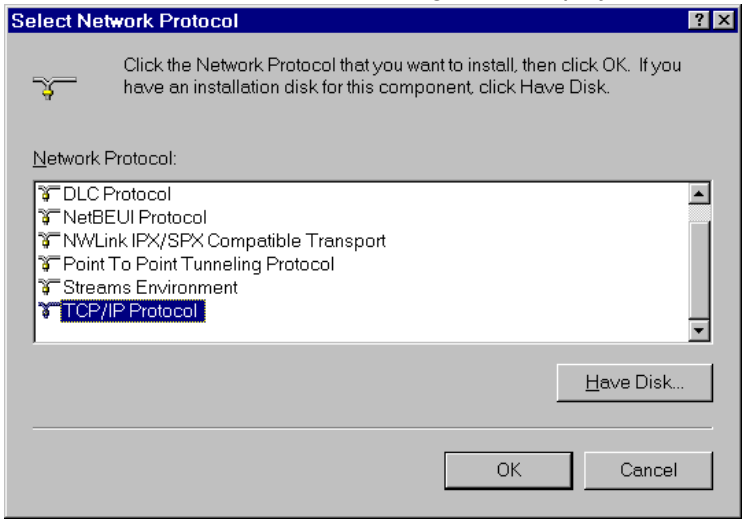
If TCP/IP is not already installed, perform the following steps:

Note: For this procedure you may need your Windows NT installation CD ROM.

1. While the **Network** dialog box is open, click **Add**.



2. The **Select Network Protocol** dialog box is displayed with a list of available protocol options.


Select Network Protocol
Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.
Network Protocol:
DLC Protocol
NetBEUI Protocol
NWLink IPX/SPX Compatible Transport
Point To Point Tunneling Protocol
Streams Environment
TCP/IP Protocol
Have Disk...
OK
Cancel

   Highlight **TCP/IP Protocol** and click **OK**.

   If necessary (e.g., the operating system does not find the necessary files on the hard drive), click the **Have Disk** button, then follow the instructions provided onscreen.

3. You are returned to the **Network** dialog.
4. Reboot your PC for changes to take effect.
5. Open the Control Panel and double-click the Network icon to return to the Network Configuration window, then go to step 4 of the **Configuring Windows NT** procedure.

ProxyServer
Internet Access / Firewall

Chapter 6 - Remote Configuration

MultiTech® Systems

Introduction

This chapter provides procedures for viewing or changing the configuration of a remote Firewall unit. Remote configuration enables a PC at one site (local site) to dial a remote Firewall and change the configuration of that remote unit. Remote configuration can be accomplished either directly through the LAN or remotely using modems. To remotely configure a Firewall, a local PC needs to be connected to a dial-up line and the Firewall software configured to call the remote Firewall. The remote Firewall needs to have a modem connected to a dial-up line and the Command Port. Once the connection to the remote unit is made, you can change the configuration as you see fit. Once the configuration is changed, you can download the new configuration to the remote Firewall.

To configure the remote Firewall through the LAN, change the communication type to the IP based Trivial File Transfer Protocol (known as TFTP) and change the configuration as you see fit. Refer to the LAN-Based Remote Configuration Procedure in this chapter to configure a remote Firewall.

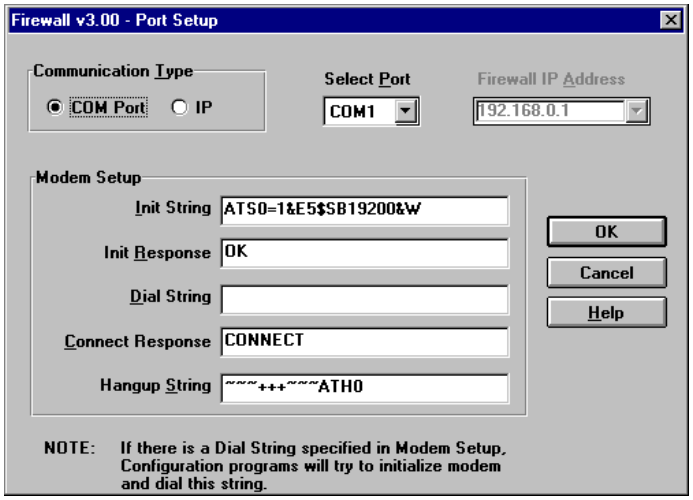
Remote Configuration

Modem-based

1. At the remote site, disconnect the serial cable from the PC to the Command port jack on the Firewall.
2. At the remote site, connect a special cable (Remote Configuration Cable) between the Command Port jack on the back panel of the Firewall and the (DB-25) RS232 connector on the modem. The special cable is a serial cable with male connectors on both ends.

   Connect the modem to your local telephone line.

   Provide your telephone number to the person verifying your configuration.
3. At the main site, connect your local PC to a modem that is connected to a dial-up line.
4. Install the Firewall software on the local PC. When installed, click **Start | Programs | Firewall Version 3.00 | Configuration Port Setup**, or double-click the **Configuration Port Setup** icon in the Firewall Version 3.00 program group.
5. The Port Setup dialog box is displayed.



Verify that the **Communication Type** is set for **COM Port** and the **Select Port** field is set for the COM port of your local PC.

In the **Dial String** field, enter the AT command for dialing (ATDT) plus the phone number of the remote Firewall.

If your Modem Initialization String, Initialization Response, or Connect Response values are different than the defaults in the dialog box, refer to your modem user documentation and change the default values to match your modem.

Click **OK** when you are satisfied with your selections.

6. Run the Proxy Server Configuration program. Click **Start | Programs | Firewall | Firewall Configuration**, or double-click the **Firewall Configuration** icon in the Firewall program group.
7. The **Dialing Router** dialog box is displayed while software is dialing the remote Firewall.
8. The **Reading Setup** dialog box is displayed.
9. The **Firewall Setup** menu is displayed. This is the dialog box of the remote Firewall. Refer to the on-line Helps provided with your software for a description of each dialog box and field within a dialog box.

10. After you have changed the configuration of the remote Firewall, click **Download Setup** to update the configuration. The remote Firewall will be brought down, the new configuration written to the unit, and the unit will reboot.
11. Click **Exit** when the downloading is complete.
12. The **Hangup connection with Router?** dialog box is displayed

    Click **Yes** to disconnect the phone connection to the remote site.
13. If the same telephone number is not going to be used again in the immediate future, you may want to remove it from the Port Setup dialog box.
14. At the remote site, reconnect the Firewall to the serial port of the PC and from the Firewall program group double-click the **Firewall Configuration** icon to verify that the Firewall is running.

LAN-based

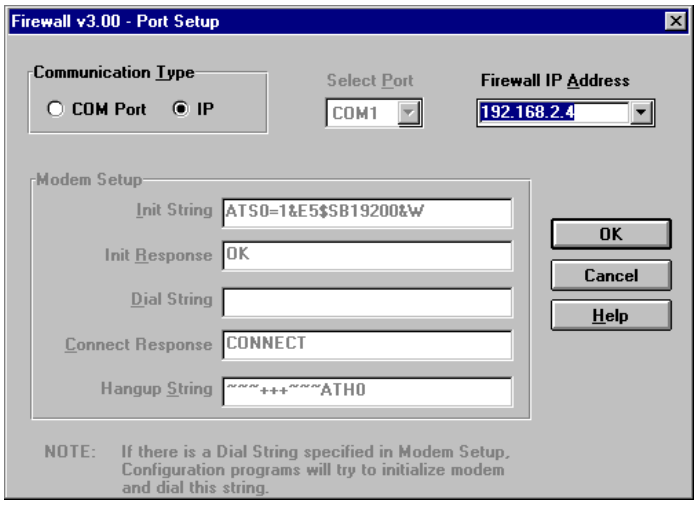
LAN-based remote configuration requires a Windows Sockets compliant TCP/IP stack. TCP/IP protocol software must be installed and functional before the configuration program can be used.

1. You must assign an Internet (IP) address for the PC and for each node that will be managed by the configuration program. Refer to the protocol software documentation for instructions on how to set the IP addresses.

   Once you have completed this step, you should be able to use the protocol Ping command for the PC host name. You should also test the network interface configuration by Pinging another TCP/IP device that is connected to the network.

2. Install the Firewall software on the local PC. When installed click **Start | Programs | Firewall Version 3.00 | Configuration Port Setup**, or double-click the **Configuration Port Setup** icon in the Firewall Version 3.00 program group.

3. The **Port Setup** dialog box is displayed.



   Verify that **IP** is selected in the **Communication Type** group.

   In the **Firewall IP Address** field, enter the IP Address of the *remote* Firewall unit.

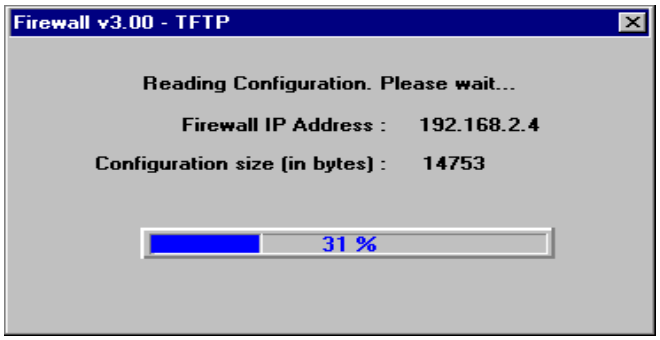
   Click **OK** when you are satisfied with your selections.

4. Run the Firewall Configuration program. Click **Start | Programs | Firewall Version 3.00 | Firewall Configuration**, or double-click the **Firewall Configuration** icon in the Firewall program group.

5. The Windows Program Manager or Desktop is displayed.

   Double-click the Firewall Configuration icon.

6. The **Reading Configuration. Please wait...** screen is displayed.


Firewall v3.00 - TFTP
Reading Configuration. Please wait...
Firewall IP Address : 192.168.2.4
Configuration size (in bytes) : 14753
31 %

7. The **Firewall Setup** main menu (for the remote Firewall unit) is then displayed. You can select any of the available buttons and change the configuration (or setup) and download the changes to the remote Firewall unit. Refer to Chapter 4 for a description of the Firewall software. For definitions of each dialog box or fields within a dialog box, refer to the Helps provided with your Firewall software.

8. After you have changed the configuration of the remote Firewall, click **Download Setup** to update the configuration. The remote Firewall will be brought down, the new configuration written to the unit, and the unit will reboot.
9. Click **Exit** when the downloading is complete.
10. Double-click the **Firewall Configuration** icon in the Program Manager screen once more to verify that the Firewall is running.

ProxyServer
Internet Access / Firewall

Chapter 7 - Firewall Management

MultiTech® Systems

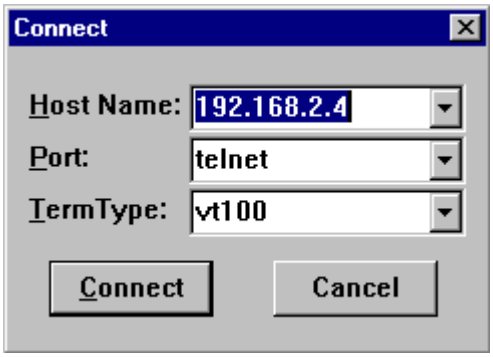
Introduction

A typical Telnet client application and typical Web-browser management of the Firewall are described in this chapter. The Firewall has a built-in Telnet Server for access through Telnet clients. A typical Telnet client is allowed to configure the Firewall and its data ports. In addition, the Firewall can be remotely accessed and configured from anywhere on the Internet through its Web interface.

For a detailed description of how the Firewall software can work in your environment, refer to Chapter 4 in this User Guide. For a detailed description of each parameter, refer to the on-line Help provided within your Firewall software.

The TCP/IP stack has to be loaded before the Telnet client can run and the Telnet Server option in the Firewall software has to be enabled. To access the Telnet Client, double click the Telnet icon. A blank Telnet screen is displayed. Click **Connect** and then **Remote System**.

When the **Connect** to remote host dialog box is displayed, a Host Name has to be entered. In this example, the IP Host Name is 192.168.2.4.

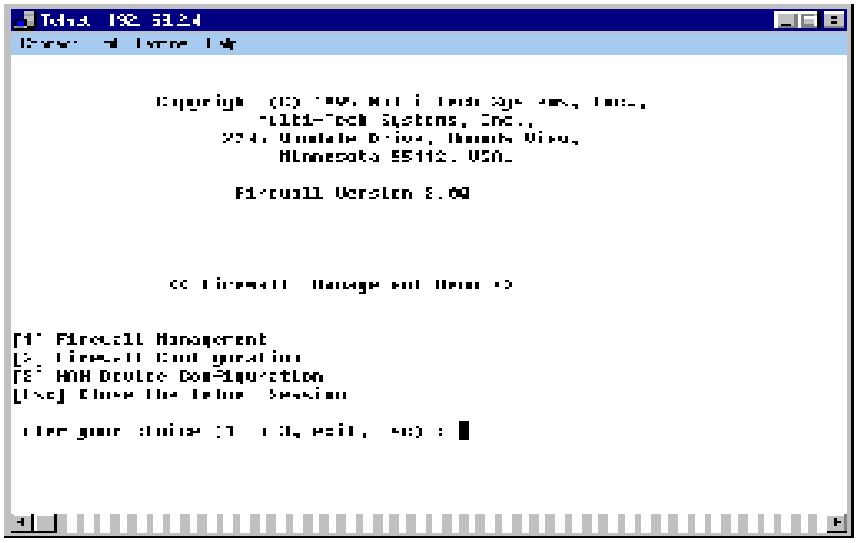


Enter your Firewall IP Address in the Host Name field. Click the **Connect** button and the Firewall Management Menu is displayed.

Firewall Management Menu

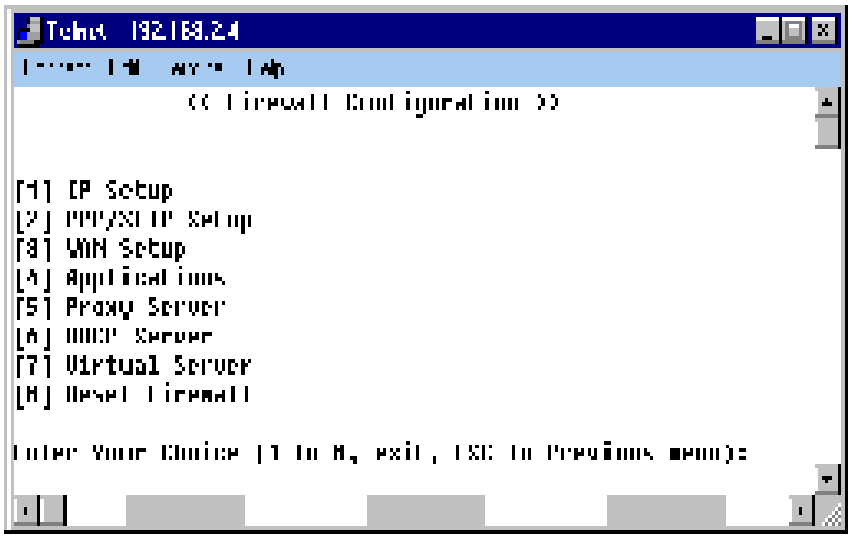
The Firewall Management Menu provides three basic options: Firewall Management, Firewall Configuration, and WAN Device Configuration. A further option enables you to close the Telnet session from this menu by pressing the Esc key.

Selecting **Option 1** displays a **Firewall Statistics** menu with options that enable you to gather various kinds of statistics or display a **System Information** screen.



Firewall Configuration

Selecting **Option 2** displays the **Firewall Configuration** menu with options that enable you to configure Firewall parameters, set up various servers, or reset the Firewall.



For more details on Firewall configuration, refer to Chapter 4 - Firewall Software, and the Helps.

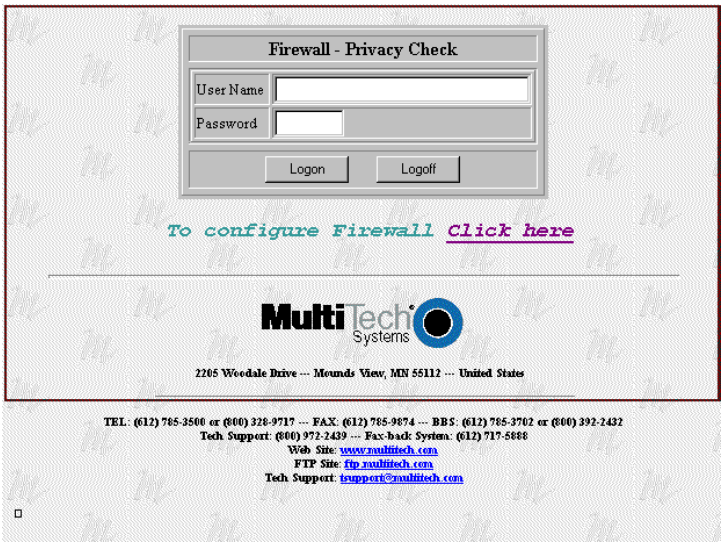
WAN Device Configuration

Selecting **Option 3** (on the **Firewall Management Menu** screen) displays the **WAN Device Configuration** options, which enable you to gain direct access to the DCE device on the WAN port.

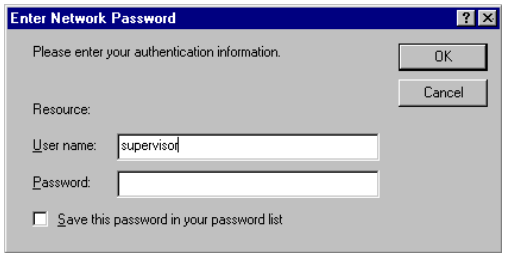
Web Browser Management

The Firewall can be accessed, via a standard Web browser, from anywhere on the connected Internet. In order to provide this support, the **WEB Server** option has to be enabled in the **Applications Setup** dialog box (see Chapter 4 - Firewall Software).

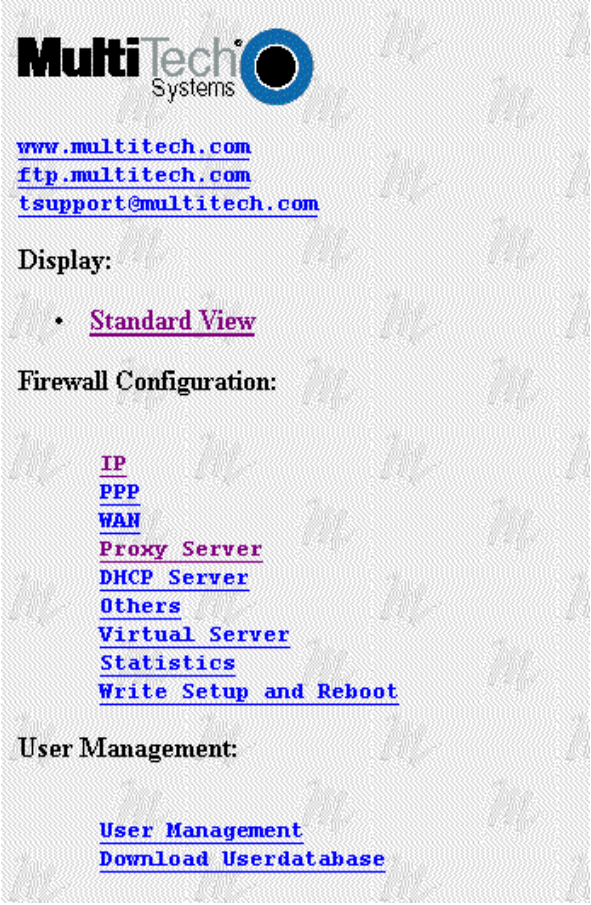
Whenever WEB Server is enabled (the default), users can access the Firewall by entering its IP address in the destination field of their Web browser. The following screen appears. The User Name and Password on this screen can be ignored, unless you have enabled and set up a username database.


Firewall - Privacy Check
User Name
Password
Logon
Logoff
To configure Firewall Click here
MultiTech Systems
2205 Woodale Drive --- Mounds View, MN 55112 --- United States
TEL: (612) 785-3500 or (800) 328-9717 --- FAX: (612) 785-9874 --- BBS: (612) 785-3702 or (800) 392-2432
Tech Support: (800) 972-2439 --- Fax-back System: (612) 717-5888
Web Site: www.multitech.com
FTP Site: ftp.multitech.com
Tech Support: tsupport@multitech.com

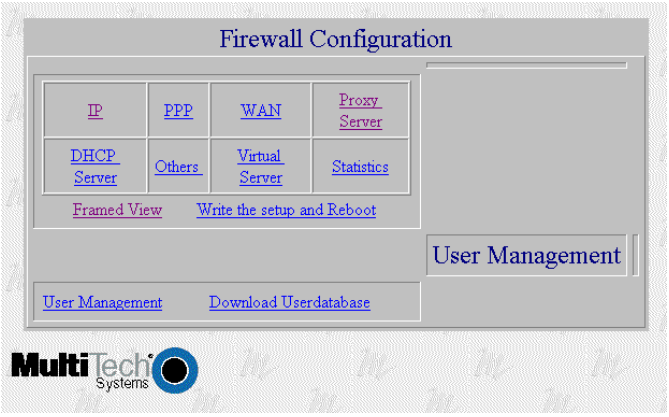
To log in to the Firewall configuration program, click the words, “click here.” The **Enter Network Password** screen is displayed.



Type **supervisor** in the **User Name** field (no password is needed), then press **Enter** or click **OK**. The default Framed View of the **Firewall Configuration** screen is displayed.



From this screen you can either access any of the configuration options or switch to the Standard View (below) to access the same options. Refer to Chapter 4 - Firewall Software for descriptions of the various options.



ProxyServer
Internet Access / Firewall

Chapter 8 - Warranty, Service and Tech Support

MultiTech® Systems

Introduction

This chapter starts out with statements about your Firewall's two-year warranty. The next section, Tech Support, should be read carefully if you have questions or problems with your Firewall. It includes the technical support telephone numbers, space for recording your product information, and an explanation of how to send in your Firewall should you require service. The final three sections explain how to use our bulletin board service (BBS), and get support through CompuServe and the Internet.

Limited Warranty

Multi-Tech Systems, Inc. ("MTS") warrants that its products will be free from defects in material or workmanship for a period of two years from the date of purchase, or if proof of purchase is not provided, two years from date of shipment. MTS MAKES NO OTHER WARRANTY, EXPRESSED OR IMPLIED, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED. This warranty does not apply to any products which have been damaged by lightning storms, water, or power surges or which have been neglected, altered, abused, used for a purpose other than the one for which they were manufactured, repaired by the customer or any party without MTS's written authorization, or used in any manner inconsistent with MTS's instructions.

MTS's entire obligation under this warranty shall be limited (at MTS's option) to repair or replacement of any products which prove to be defective within the warranty period, or, at MTS's option, issuance of a refund of the purchase price. Defective products must be returned by Customer to MTS's factory transportation prepaid.

MTS WILL NOT BE LIABLE FOR CONSEQUENTIAL DAMAGES AND UNDER NO CIRCUMSTANCES WILL ITS LIABILITY EXCEED THE PURCHASE PRICE FOR DEFECTIVE PRODUCTS.

On-line Warranty Registration

To register your Firewall on-line, click the following link:

http://www.multitech.com/register

Scroll down, then enter your Firewall's serial number; select "ProxyServer" and "MTPSR1-120," then, enter the additional information needed to complete the registration form.

Tech Support

Multi-Tech has an excellent staff of technical support personnel available to help you get the most out of your Multi-Tech product. If you have any questions about the operation of this unit, call 1-800-972-2439. Please fill out the Firewall information (below), and have it available when you call. If your Firewall requires service, the tech support specialist will guide you on how to send in your Firewall (refer to the next section).

Recording Firewall Information

Please fill in the following information on your Multi-Tech Firewall. This will help tech support in answering your questions. (The same information is requested on the Warranty Registration Card.)

Model No.: _____
Serial No.: _____
Software Version: _____

The model and serial numbers are on the bottom of your Firewall.

Note the type of WAN device (if any) that is connected to the RS232/V.35 connector on the back panel of your Firewall before calling tech support. Also, note the status of your Firewall including LED indicators, screen messages, diagnostic test results, problems with a specific application, etc. Use the space below to note the Firewall status:

_____

_____

_____

_____

_____

_____

_____

_____

Service

If your tech support specialist decides that service is required, your Firewall may be sent (freight prepaid) to our factory. Return shipping charges will be paid by Multi-Tech Systems.

Include the following with your Firewall:

- a description of the problem.
- return billing and return shipping addresses.
- contact name and phone number.
- check or purchase order number for payment if the Firewall is out of warranty. (Check with your technical support specialist for the standard repair charge for your Firewall).
- if possible, note the name of the technical support specialist with whom you spoke.

If you need to inquire about the status of the returned product, be prepared to provide the **serial number** of the product sent.

Send your Firewall to this address:

MULTI-TECH SYSTEMS, INC.

2205 WOODALE DRIVE

MOUNDS VIEW, MINNESOTA 55112

ATTN: SERVICE OR REPAIRS

You should also check with the supplier of your Firewall on the availability of local service and/or loaner units in your part of the country.

About the Internet

Multi-Tech is a commercial user on the Internet, and we retrieve messages from our customers on a periodic basis. Multi-Tech's presence includes a Web site at:

http://www.multitech.com

and an FTP site at:

ftp://ftp.multitech.com

Ordering Accessories

SupplyNet, Inc. supplies replacement transformers, cables and connectors for select Multi-Tech products. You can place an order with SupplyNet via mail, phone, fax or the Internet at:

Mail: SupplyNet, Inc.
614 Corporate Way
Valley Cottage, NY 10989

Phone: 800 826-0279

Fax: 914 267-2420

Email: info@thesupplynet.com

Internet: http://www.thesupplynet.com

ProxyServer
Internet Access / Firewall

Appendixes

MultiTech® Systems

Appendix A - TCP/IP (Transmission Control Protocol/ Internet Protocol) Description

TCP/IP is a protocol suite and related applications developed for the U.S. Department of Defense in the 1970s and 1980s specifically to permit different types of computers to communicate and exchange information with one another. TCP/IP is currently mandated as an official U.S. Department of Defense protocol and is also widely used in the UNIX community.

Before you install TCP/IP on your network, you need to establish your Internet addressing strategy. First, choose a domain name for your company. A domain name is the unique Internet name, usually the name of your business, that identifies your company. For example, Multi-Tech's domain name is multitech.com (.com indicates this is a commercial organization; .edu denotes educational organizations, .gov denotes government organizations). Next, determine how many IP addresses you'll need. This depends on how many individual network segments you have, and how many systems on each segment need to be connected to the Internet. You'll need an IP address for each network interface on each computer and hardware device.

IP addresses are 32 bits long and come in two types: network and host. Network addresses come in five classes: A, B, C, D, and E. Each class of network address is allocated a certain number of host addresses. For example, a class B network can have a maximum of 65,534 hosts, while a class C network can have only 254. The class A and B addresses have been exhausted, and the class D and E addresses are reserved for special use. Consequently, companies now seeking an Internet connection are limited to class C addresses.

Early IP implementations ran on hosts commonly interconnected by Ethernet local area networks (LAN). Every transmission on the LAN contains the local network, or medium access control (MAC), address of the source and destination nodes. The MAC address is 48-bits in length and is non-hierarchical; MAC addresses are never the same as IP addresses.

When a host needs to send a datagram to another host on the same network, the sending application must know both the IP and MAC addresses of the intended receiver. Unfortunately, the IP process may not know the MAC address of the receiver. The Address Resolution Protocol (ARP), described in RFC 826 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc826.txt) provides a mechanism for a host to determine a receiver's MAC address from the IP address. In the process, the host sends an ARP packet in a frame containing the MAC broadcast address; and then the ARP request advertises the destination IP address and asks for the associated MAC address. The station on the LAN that recognizes its own IP address will send an ARP response with its own MAC address. An ARP message is carried directly in an IP datagram.

Other address resolution procedures have also been defined, including those which enable a diskless processor to determine its IP address from its MAC address (Reverse ARP, or RARP), provides a mapping between an IP address and a frame relay virtual circuit identifier (Inverse ARP, or InARP), and provides a mapping between an IP address and ATM virtual path/channel identifiers (ATMARP).

The TCP/IP protocol suite comprises two protocols that correspond roughly to the OSI Transport and Session Layers; these protocols are called the Transmission Control Protocol and the User Datagram Protocol (UDP). Individual applications are referred to by a port identifier in TCP/UDP messages. The port identifier and IP address together form a "socket". Well-known port numbers on the server side of a connection include 20 (FTP data transfer), 21 (FTP control), 23 (Telnet), 25 (SMTP), 43 (whois), 70 (Gopher), 79 (finger), and 80 (HTTP).

TCP, described in RFC 793 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc793.txt) provides a virtual circuit (connection-oriented) communication service across the network. TCP includes rules for formatting messages, establishing and terminating virtual circuits, sequencing, flow control, and error correction. Most of the applications in the TCP/IP suite operate over the "reliable" transport service provided by TCP.

UDP, described in RFC 768 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc768.txt) provides an end-to-end datagram (connectionless) service. Some applications, such as those that involve a

simple query and response, are better suited to the datagram service of UDP because there is no time lost to virtual circuit establishment and termination. UDP's primary function is to add a port number to the IP address to provide a socket for the application.

The Application Layer protocols are examples of common TCP/IP applications and utilities, which include:

- Telnet (Telecommunication Network): a virtual terminal protocol enableing a user logged on to one TCP/IP host to access other hosts on the network, described in RFC 854 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc854.txt).
- FTP: the File Transfer Protocol enables a user to transfer files between local and remote host computers per RFC 959 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc959.txt).
- Archie: a utility that enables a user to search all registered anonymous FTP sites for files on a specified topic.
- Gopher: a tool that enables users to search through data repositories using a menu-driven, hierarchical interface, with links to other sites, per RFC 1436 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1436.txt).
- SMTP: the Simple Mail Transfer Protocol is the standard protocol for the exchange of electronic mail over the Internet, per RFC 821 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc821.txt).
- HTTP: the Hypertext Transfer Protocol is the basis for exchange of information over the World Wide Web (WWW). Various versions of HTTP are in use over the Internet, with HTTP version 1.0, per RFC 1945 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1945.txt) being the most current.
- HTML: WWW pages are written in the Hypertext Markup Language (HTML), an ASCII-based, platform-independent formatting language, per RFC 1866 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1866.txt).
- Finger: used to determine the status of other hosts and/or users, per RFC 1288 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1288.txt).
- POP: the Post Office Protocol defines a simple interface between a user's mail reader software and an electronic mail server; the current version is POP3, described in RFC 1460 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1460.txt).
- DNS: the Domain Name System defines the structure of Internet names and their association with IP addresses, as well as the association of mail, name, and other servers with domains.
- SNMP: the Simple Network Management Protocol defines procedures and management information databases for managing TCP/IP-based network devices. SNMP, defined by RFC 1157 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1157.txt) is widely deployed in local and wide area network. SNMP Version 2 (SNMPv2), per RFC 1441 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1441.txt) adds security mechanisms that are missing in SNMP, but is also more complex.
- Ping: a utility that enables a user at one system to determine the status of other hosts and the latency in getting a message to that host. Ping uses ICMP Echo messages.
- Whois/NICNAME: Utilities that search databases for information about Internet domain and domain contact information, per RFC 954 (http://info.internet.isi.edu:80/in-notes/rfc/files/rfc954.txt).
- Traceroute: a tool that displays the route that packets will take when traveling to a remote host.

Internet Protocol (IP)

IP is the Internet standard protocol that tracks Internetwork node addresses, routes outgoing messages and recognizes incoming messages, enabling a message to cross multiple networks on the way to its final destination. The IPv6 Control Protocol (IPV6CP) is responsible for configuring, enabling, and disabling the IPv6 protocol modules on both ends of the point-to-point link. IPV6CP uses the same packet exchange mechanism as the Link Control Protocol (LCP). IPV6CP packets are not exchanged until PPP has reached the Network-Layer Protocol phase. IPV6CP packets received before this phase is reached are silently discarded. (See also TCP/IP.)

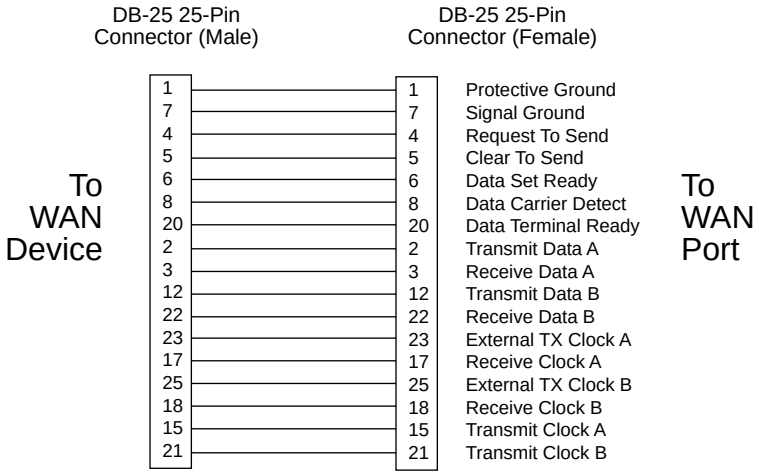
Before you install TCP/IP on your network, you need to establish your Internet addressing strategy. You first choose a domain name for your company. A domain name is the unique Internet name, usually the name of your business, that identifies your company. For example, Multi-Tech's domain name is multitech.com (where .com indicates this is a commercial organization; .edu denotes educational organizations, .gov denotes government organizations). Next, you determine how many IP addresses you'll need. This depends on how many individual network segments you have, and how many systems on each segment need to be connected to the Internet. You need an IP address for each network interface on each computer and hardware device.

IP addresses are 32 bits long and come in two types: network and host. Network addresses come in five classes: A, B, C, D, and E. Each class of network address is allocated a certain number of host addresses. For example, a class B network can have a maximum of 65,534 hosts, while a class C network can have only 254. The class A and B addresses have been exhausted, and the class D and E addresses are reserved for special use. Consequently, companies now seeking an Internet connection are limited to class C addresses. The current demand for Internet connections will exhaust the current stock of 32-bit IP addresses. In response, Internet architects have proposed the next generation of IP addresses, Ipng (IP Next Generation). It will feature 16-byte addressing, surpassing the capacities of 32-bit IP. Still in its design phase, IPng is not expected to be widely deployed before late 1997.

An IP address can serve only a single physical network. Therefore, if your organization has multiple physical networks, you must make them appear as one to external users. This is done via "subnetting", a complex procedure best left to ISPs and others experienced in IP addressing. Since IP addresses and domain names have no inherent connection, they are mapped together in databases stored on Domain Name Servers (DNS). If you decide to let an Internet Service Provider (ISP) administer your DNS server, the ISP can assist you with the domain name and IP address assignment necessary to configure your company's site-specific system information. Domain names and IP addresses are granted by the InterNIC. To check the availability of a specific name or to obtain more information, call the InterNIC at (703)742-4777, or visit the InterNIC web site at http://www.internic.com.

Appendix B - Cabling Diagrams

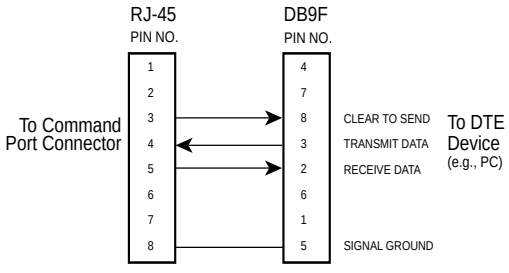
WAN Port Cable (RS-232/V.35)



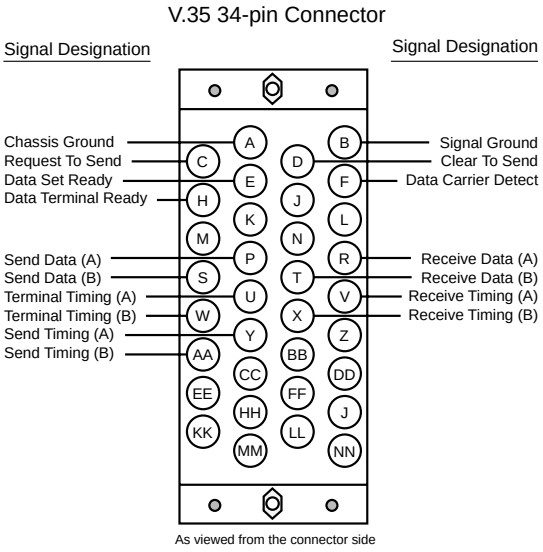
Ethernet Cables (10BaseT)

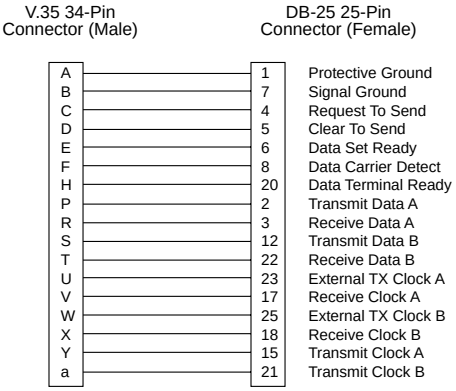
Pin		Circuit Signal Name
1	TD+	Data Transmit Positive
2	TD-	Data Transmit Negative
3	RD+	Data Receive Positive
6	RD-	Data Receive Negative

Command Port Cable (RJ-45)



DB-25 (RS-232) to V.35 Adapter

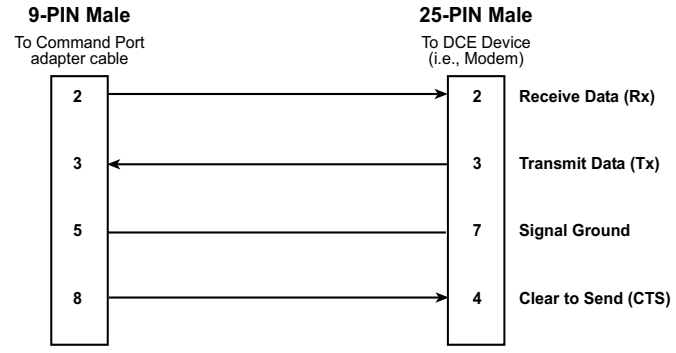



V.35 34-Pin Connector (Male)
DB-25 25-Pin Connector (Female)
A 1 Protective Ground
B 7 Signal Ground
C 4 Request To Send
D 5 Clear To Send
E 6 Data Set Ready
F 8 Data Carrier Detect
H 20 Data Terminal Ready
P 2 Transmit Data A
R 3 Receive Data A
S 12 Transmit Data B
T 22 Receive Data B
U 23 External TX Clock A
V 17 Receive Clock A
W 25 External TX Clock B
X 18 Receive Clock B
Y 15 Transmit Clock A
a 21 Transmit Clock B

* The RS-232C Interface circuits have been designed to meet the electrical specifications given in EIA (Electronic Industries Association) RS-232C and CCITT (Consultive Committee International Telegraph and Telephone) V.24 Standards

** When configured for V.35 interface operation on the link, the V.35 adapter cable should be used. This cable uses a 25-pin female connector at one end and a 34-pin winchester male connector at the other.

Remote Configuration Cable


9-PIN Male
To Command Port adapter cable
25-PIN Male
To DCE Device (i.e., Modem)
2 2 Receive Data (Rx)
3 3 Transmit Data (Tx)
5 7 Signal Ground
8 4 Clear to Send (CTS)

Appendix C - Script Commands

A script file can be used to automate certain operations. The script file is a text file containing a sequence of the following commands (listed here according to their functions). This is similar to what you will find in the Help file in your Firewall software. Following the list of commands is an example script.

Commands (by Function)

Dial, Connection and Remote

ACTIVATEDOD	BAUDRATE	BREAK
GETCTS	GETDCD	HANGUP
PARITYR	GETC	RGETS
RXFLUSH	SETDTR	SETRTS
STOPBITS	THISLAYERUP	TRANSMIT
TXFLUSH	WAITFOR	

Mathematical functions

DEC	INC

Miscellaneous

EXIT	WAIT

Program constructs

FOR	IF	PROC
SWITCH	WHILE	

String operations

ATOI	ITOA	STRCAT
STRCMP	STRCOPY	STRFMT
STRLEN	TOLOWER	TOUPPER

Example Script:

```
proc main;
      string login_prompt;
      string user_name;
      string password_prompt;
      string password;
      string shell_menu;
      string shell_menu_response;
      integer timeout;

      timeout=10;
      login_prompt=”login:”;
      user_name=”user1”;
      password_prompt=”Password:”;
      password=”user1”;
      shell_menu=”choice:”;
      shell_menu_response=”1”;

      transmit(“A”);
      wait(1)
      transmit(“T^M”);
      waitfor (“OK”,10);

      transmit (“A”);
      wait (1);
      transmit (“T”);
      wait (1);
      transmit (“DT963^M”);

      if (waitfor (login_prompt,60))  then
          transmit (user_name);
          transmit (“^M”);
          if (waitfor (password_prompt,timeout))  then
                transmit (password);
                transmit (“^M”);
                 if (waitfor (shell_menu,timeout))  then
                        transmit (shell_menu_response);
                       transmit (“^M”);
        else
                        transmit (“Shell Menu Not Received^M”);
        endif
      else
        transmit (“Password Prompt Not Received^M”);
        endif
      else
        transmit (“Login Prompt Not Received^M”);
      endif

Endproc
```

Appendix D - Regulatory Information

FCC Declaration

NOTE: This equipment has been tested and found to comply with the limits for a **Class A** digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

EMC and Safety Directive Compliance

CE

The CE mark is affixed to this Multi-Tech product to confirm compliance with the following European Community Directives:

Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of Member States relating to electromagnetic compatibility.

and

Council Directive 73/23/EEC of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits:

each amended by

Council Directive 93/68/EEC of 22 July 1993 on the harmonization of CE marking requirements.

ProxyServer

Internet Access / Firewall

Glossary of Terms

MultiTech® Systems

A

Access: The T1 line element made up of two pairs of wire that the telephone company brings to the customer premises. The Access portion ends with a connection at the local telco (LEC or RBOC).

Accunet Spectrum of Digital Services (ASDS): The AT&T 56 Kbps leased (private) line service. Similar to services of MCI and Sprint. ASDS is available in nx56/64 Kbps, where n=1, 2, 4, 6, 8, 12.

ACK (ACKnowledgement code) (pronounced “ack”): A communications code sent from a receiving modem to a transmitting modem to indicate that it is ready to accept data. It is also used to acknowledge the error-free receipt of transmitted data. Contrast with NAK.

Adaptive Differential Pulse Code (ADCPM): In multimedia applications, a technique in which pulse code modulation samples are compressed before they are stored on a disk. ADCPM, an extension of the PCM format, is a standard encoding format for storing audio information in a digital format. It reduced storage requirements by storing differences between successive digital samples rather than full values.

Address: A numbered location inside a computer. It’s how the computer accesses its resources, like a video card, serial ports, memory, etc.

AMI line coding: One of two common methods of T1 line coding (with B8ZS). AMI line coding places restrictions on user data (B8ZS does not).

Analog signal: A waveform which has amplitude, frequency and phase, and which takes on a range of values between its maximum and minimum points.

Analog Transmission: One of two types of telecommunications which uses an analog signal as a carrier of voice, data, video, etc. An analog signal becomes a carrier when it is modulated by altering its phase, amplitude and frequency to correspond with the source signal. Compare with digital transmission.

Application Program Interface (API): A software module created to allow dissimilar, or incompatible applications programs to transfer information over a communications link. APIs may be simple or complex; they are commonly required to link PC applications with mainframe programs.

ASCII (American Standard Code for Information Interchange) (pronounced “askey”): A binary code for data that is used in communications and in many computers and terminals. The code is used to represent numbers, letters, punctuation and control characters. The basic ASCII code is a 7-bit character set which defines 128 possible characters. The extended ASCII file provides 255 characters.

Asynchronous Transfer Mode (ATM): A very high-speed method of transmission that uses fixed-size cells of 53 bytes to transfer information over fiber; also known as cell relay.

AT Commands: A standard set of commands used to configure various modem parameters, establish connections and disconnect. The “AT” is used to get the “attention” of the modem before the actual command is issued.

Availability: The measure of the time during which a circuit is ready for use; the complement of circuit “outage” (100% minus % outage = % available).

B

B7ZS (Bipolar 7 Zero Suppression) line coding: One method of T1 line coding (see also “B8ZS” and “AMI”). B7ZS line coding does not place restrictions on user data (AMI does).

B8ZS (Bipolar 8 Zero Suppression) line coding: One of two common methods of T1 line coding (with AMI). B8ZS line coding does not place restrictions on user data (AMI does). A coding method used to produce 64 Kbps “clear” transmission. (See also “B7ZS” and “AMI” line coding)

Backbone: 1. A set of nodes and their interconnecting links providing the primary data path across a network. 2. In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges. A backbone may be configured as a bus or as a ring. 3. In a wide area network, a high-speed link to which nodes or data switching exchanges (DSEs) are connected. 4. A common distribution core that provides all electrical power, gases, chemicals, and other services to the sectors of an automated wafer processing system.

Background: An activity that takes place in the PC while you are running another application. In other words, the active user interface does not correspond to the ‘background’ task.

Bandwidth: The transmission capacity of a computer channel, communications line or bus. It is expressed in cycles per second (hertz), the bandwidth being the difference between the lowest and highest frequencies transmitted. The range of usable frequencies that a transmission medium will pass without unacceptable attenuation or distortion. Bandwidth is a factor in determining the amount of information and the speed at which a medium can transmit data or other information.

Backward Explicit Congestion Notification (BECN): A bit that tells you that a certain frame on a particular logical connection has encountered heavy traffic. The bit provides notification that congestion-avoidance procedures should be initiated in the opposite direction of the received frame. See also FECN (Forward Explicit Congestion Notification).

Basic Rate Interface (BRI): An ISDN access interface type comprised of two B-channels each at 64 Kbps and one D-channel at 64 Kbps (2B+D).

Bell Operating Companies (BOC): The family of corporations created during the divestiture of AT&T. BOCs are independent companies which service a specific region of the US. Also called Regional Bell Operating Companies (RBOCs).

Bell Pub 41450: The Bell publication defining requirements for data format conversion, line conditioning, and termination for direct DDS connection.

Bell Pub 62310: The Bell publication defining requirements for data format conversion, line conditioning, and termination for direct DDS connection.

Binary Synchronous Communication (BSC): A form of telecommunication line control that uses a standard set of transmission control characters and control character sequences, for binary synchronous transmission of binary-coded data between stations.

Bit (Binary digIT): A bit is the basis of the binary number system. It can take the value of 1 or 0. Bits are generally recognized as the electrical charge generated or stored by a computer that represent some portion of usable information.

Bit Error Rate Test (BERT): A device or routine that measures the quality of data transmission. A known bit pattern is transmitted, and the errors received are counted and a BER (bit error rate) is calculated. The BER is the ratio of received bits in error relative to the total number of bits received, expressed in a power of 10.

Bit robbing: The use of the least significant bit per channel in every sixth frame for signaling. The line signal bits “robbed” from the speech part conveys sufficient pre-ISDN telephony signaling information with the remaining line signal bits providing sufficient line signaling bits for recreating the original sound. See “robbed bit signaling”.

Blue Alarm: An error indication signal consisting of all 1s indicating disconnection or attached device failure. Contrast “Red Alarm” and “Yellow Alarm”.

Bps (bits per second): A unit to measure the speed at which data bits can be transmitted or received. Bps differs from baud when more than one bit is represented by a single cycle of the carrier.

Bridges: 1. A functional unit that interconnects two local area networks that use the same logical link protocol but may use different medium access control protocols. 2. A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address. 3. In the connection of local loops, channels, or rings, the equipment and techniques used to match circuits and to facilitate accurate data transmission.

Buffer: A temporary storage register or Random Access Memory (RAM) used in all aspects of data communications which prevents data from being lost due to differences in transmission speed. Keyboards, serial ports, muxes and printers are a few examples of the devices that contain buffers.

Bus: A common channel between hardware devices either internally between components in a computer, or externally between stations in a communications network.

Byte: The unit of information a computer can handle at one time. The most common understanding is that a byte consists of 8 binary digits (bits), because that’s what computers can handle. A byte holds the equivalent of a single character (such as the letter A).

C

Call Setup Time: The time to establish a circuit-switched call between two points. Includes dialing, wait time, and CO/long distance service movement time.

Carrier Group Alarm (CGA): A T1 service alarm generated by a channel bank when an OOF condition occurs for a predefined length of time (usually 300mS to 2.5 seconds). The CGA causes the calls using a trunk to be dropped and for trunk conditioning to be applied.

Carrier signal: An analog signal with known frequency, amplitude and phase characteristics used as a transport facility for useful information. By knowing the original characteristics, a receiver can interpret any changes as modulations, and thereby recover the information.

CCITT (Consultative Committee for International Telephone and Telegraph): An advisory committee created and controlled by the United Nations and headquartered in Geneva whose purpose is to develop and to publish recommendations for worldwide standardization of telecommunications devices. CCITT has developed modem standards that are adapted primarily by PTT (post telephone and telegraph) organizations that operate telephone networks of countries outside of the U.S. See also ITU.

Central Office (CO): The lowest, or most basic level of switching in the PSTN (public switched telephone network). A business PABX or any residential telephone connects to the PSTN at a central office.

Centrex: A multi-line service offered by operating Telcos which provides, from the Telco CO, functions and features comparable to those of a PBX for large business users. See also “Private Branch Exchange”, “Exchange”.

Channel: A data communications path between two computer devices. Can refer to a physical medium (e.g., UTP or coax), or to a specific carrier frequency.

Channel Bank: A device that acts as a converter, taking the digital signal from the T1 line into a phone system and converting it to the analog signals used by the phone system. A channel bank acts as a multiplexer, placing many slow-speed voice or data transactions on a single high-speed link.

CHAP (Challenge-Handshake Authentication Protocol): An authentication method that can be used when connecting to an Internet Service Provider. CHAP allows you to log in to your provider automatically, without the need for a terminal screen. It is more secure than Password Authentication Protocol (See PAP) since it does not send passwords in text format.

Circuit-switched Network: A technology used by the PSTN that allocates a pair of conductors for the exclusive use of one communication path. Circuit switching allows multiple conversations on one talk path only if the end-users multiplex the signals prior to transmission.

Circuit Switching: The temporary connection of two or more communications channels using a fixed, non-shareable path through the network. Users have full use of the circuit until the connection is terminated.

Clear Channel: A transmission path where the full bandwidth is used (i.e., no bandwidth needed for signaling, carrier framing or control bits). A 64 Kbps digital circuit usually has 8 Kbps used for signaling. ISDN has two 64 Kbps circuits, and a 16 Kbps packet service of which part is used for signaling on the 64K channels.

Client-Server: In TCP/IP, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

Cluster Controller: A device that can control the input/output operations of more than one device connected to it. A cluster controller may be controlled by a program stored and executed in the unit, or it may be entirely controlled by hardware.

Committed Burst Size: The maximum number of bits that the frame relay network agrees to transfer during any measurement interval.

Committed Information Rate (CIR): An agreement a customer makes to use a certain minimum data transmission rate (in bps). The CIR is part of the frame relay service monthly billing, along with actual usage, that users pay to their frame relay service provider.

Compression: 1. The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks. 2. In SNA, the replacement of a string of up to 64 repeated characters by an encoded control byte to reduce the length of the data stream to the LU-LU session partner. The encoded control byte is followed by the character that was repeated (unless that character is the prime compression character). 3. In Data Facility Hierarchical Storage Manager, the process of moving data instead of allocated space during migration and recall in order to release unused space. 4. Contrast with decompression.

COMx Port: A serial communications port on a PC.

Congestion: A network condition where there is too much data traffic. The ITU I.233 standard defines congestion management in terms of speed and burstiness.

Congestion notification: The function in frame relay that ensures that user data transmitted at a rate higher than the CIR are allowed to slow down to the rate of the available network bandwidth.

Consecutive Severely Errored Seconds (CSES): An error condition that occurs when from 3 to 9 SES (Severely Errored Seconds) are logged consecutively.

Customer Premise Equipment (CPE): The generic term for data comm and/or terminal equipment that resides at the user site and is owned by the user with the following exclusions: Over voltage protection equipment, inside wiring, coin operated or pay telephones, “company-official” equipment, mobile telephone equipment, “911” equipment, equipment necessary for the provision of communications for national defense, or multiplexing equipment used to deliver multiple channels to the customer.

D

D4: the T1 4th generation channel bank.

D4 channelization: Refers to the compliance with AT&T TR 62411 for DS1 frame layout.

D4 framing: The T1 format for framing in AT&T D-Series channel banks, in which there are 12 separate 193-bit frames in a Superframe. A D4 framing bit is used to identify the channel and the signaling frame. Signalling for voice channels is carried in-band for every channel, along with the encoded voice. See “robbed-bit signaling”.

Data Communications Equipment (DCE): Any device which serves as the portal of entry from the user equipment to a telecommunications facility. A modem is a DCE for the telephone network (PSTN) that is commonly on site at the user’s premises. Packet Switched Networks have another level of DCE which is most often located at a central office.

Data Link Connection Identifier (DLCI): One of the six components of a frame relay frame. Its purpose is to distinguish separate virtual circuits across each access connection. Data coming into a frame relay node is thus allowed to be sent

across the interface to the specified “address”. The DLCI is confirmed and relayed to its destination, or if the specification is in error, the frame is discarded.

Data Terminal Ready (DTR): A control signal sent from the DTE to the DCE that indicates that the DTE is powered on and ready to communicate.

Dataphone Digital Service (DDS): A private line digital service that offers 2400, 4800, 9600 and 56 Kbps data rates on an inter-LATA basis by AT&T and on an intra-LATA basis by the BOCs.

Data Service Unit (DSU): A device that provides a digital data service interface directly to the data terminal equipment. The DSU provides loop equalization, remote and local testing capabilities, and a standard EIA/CCITT interface.

Dedicated Line: A communication line that is not switched. The term leased line is more common.

Default: This is a preset value or option in software packages, or in hardware configuration, that is used unless you specify otherwise.

Device driver: Software that controls how a computer communicates with a device, such as a printer or mouse.

Digital Cross-connect System (DCS): The CO device which splits and redistributes the T1 bandwidth. The DCS takes time slots from various T1 lines and alters them to provide the needed connectivity. DCS connections are made with software at an administrator’s workstation.

Digital Data: Information represented by discrete values or conditions (contrast “Analog Data”).

Digital Loopback: A technique used for testing the circuitry of a communications device. Can be initiated locally, or remotely (via a telecommunications device). The tested device decodes and encodes a received test message, then echoes the message back. The results are compared with the original message to determine if corruption occurred en route.

Digital PBX: A Private Branch Exchange that operates internally on digital signals. See also “Exchange”.

Digital Service, level 0 (DS0): The worldwide standard speed (64 Kbps) for digital voice conversation using PCM (pulse coded modulation).

Digital Service, level 1 (DS1): The 1.544 Mbps voice standard (derived from an older Bell System standard) for digitized voice transmission in North America. The 1.544 Mbps consists of 24 digitally-encoded 64 Kbps voice channels (north America) and 2.048 Mbps (30 channels) elsewhere.

Digital Signal: A discrete or discontinuous signal (e.g., a sequence of voltage pulses). Digital devices, such as terminals and computers, transmit data as a series of electrical pulses which have discrete jumps rather than gradual changes.

Digital Signaling Rates (DSn): A hierarchical system for transmission rates, where “DS0” is 64 Kbps (equivalent to ISDN B channel), and DS1 is 1.5 Mbps (equivalent to ISDN PRI).

Digital Transmission: A method of electronic information transmission common between computers and other digital devices. Analog signals are waveforms: a combination of many possible voltages. A computer’s digital signal may be only “high” or “low” at any given time. Therefore, digital signals may be “cleaned up” (noise and distortion removed) and amplified during transmission.

Digitize: To convert an analog signal to a digital signal.

DIP switch (pronounced “dip switch”): A set of tiny toggle switches, built into a DIP (dual in-line package), used for setting configurable parameters on a PCB (printed circuit board).

Domain Name Server (DNS): Also known as “resolvers”, are a system of computers which convert domain names into IP addresses, which consist of a string of four numbers up to three digits each. Each applicant for a domain name must provide both a primary and a secondary DNS server; a domain name which fails to provide both primary and secondary DNS servers is known as a “lame delegation.”

Driver: A software module that interfaces between the Operating System and a specific hardware device (e.g., color monitors, printers, hard disks, etc.). Also known as a device driver.

Drop and Insert: The process where a portion of information carried in a transmission system is demodulated (“Dropped”) at an intermediate point and different information is included (“Inserted”) for subsequent transmission.

DTE (Data Terminal Equipment): A term used to include any device in a network which generates, stores or displays user information. DTE is a telecommunications term which usually refers to PCs, terminals, printers, etc.

DTMF (Dual-Tone MultiFrequency): A generic push-button concept made popular by AT&T TouchTone.

Dynamic Host Configuration Protocol (DHCP): An IETF protocol which allows a server to dynamically assign IP addresses to Nodes (workstations). DHCP supports manual, automatic and dynamic address assignment; provides client information including the subnetwork mask, gateway address; and is routable. A DHCP server, generally a dedicated server, verifies the device’s identity, “leases” an IP address for a predetermined period of time and reclaims the address upon expiration for reassignment to another workstation.

E

E&M: A telephony trunking system used for either switch-to-switch, or switch-to-network, or computer/telephone system-to-switch connection.

EIA: The Electronics Industries Association is a trade organization in Washington, DC that sets standards for use of its member companies. (See RS-232, RS-422, RS530.)

Encapsulation: A technique used by network-layer protocols in which a layer adds header information to the protocol data unit from the preceding layer. Also used in “enveloping” one protocol inside another for transmission. For example, IP inside IPX.

Errored Seconds (ES): Any second of operation that all 1.544M bits are not received exactly as transmitted. Contrast “Error Free Seconds”.

Error Free Seconds (EFS): Any second of operation that all 1.544M bits are received exactly as transmitted. Contrast “Errored Seconds”.

ESF Error Event: A T1 error condition that is logged when a CRC-6 error or an Out-Of-Frame (OOF) error occurs.

Ethernet: A 10-megabit baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and transmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

Excess Zeros: A T1 error condition that is logged when more than 15 consecutive 0s or fewer than one 1 bit in 16 bits occurs.

Exchange: A unit (public or private) that can consist of one or more central offices established to serve a specified area. An exchange typically has a single rate of charges (tariffs) that has previously been approved by a regulatory group.

Exchange Area: A geographical area with a single uniform set of charges (tariffs), approved by a regulatory group, for telephone services. Calls between any two points within an exchange area are local calls. See also “Digital PBX”, “PBX”.

Exchange Termination (ET): The carrier’s local exchange switch. Contrast with “Loop Termination - LT”.

Explicit Congestion Management: The method used in frame relay to notify the terminal equipment that the network is overly busy. The use of FECN and BECN is called explicit congestion management. Some end-to-end protocols use FECN or BECN, but usually not both options together. With this method, a congestion condition is identified and fixed before it becomes critical. Contrast with “implicit congestion”.

Extended Super Frame (ESF): One of two popular formats for framing bits on a T1 line. ESF framing has a 24-frame Superframe, where robbed bit signaling is inserted in the LSB (bit 8 of the DS-0 byte) of frames 6, 12, 18 and 24. ESF has more T1 error measurement capabilities than D4 framing. Both ESF and B8ZS are typically offered to provide clear channel service.

F

Failed Seconds: A test parameter where the circuit is unavailable for one full second.

Failed Signal: A T1 test parameter logged when there are more than 9 SES (Severely Errored Seconds).

Fax (facsimile): Refers to the bit-mapped rendition of a graphics-oriented document (fax) or to the electronic transmission of the image over telephone lines (faxing). Fax transmission differs from data transmission in that the former is a bit-mapped approximation of a graphical document and, therefore, cannot be accurately interpreted according to any character code.

Firmware: A category of memory chips that hold their content without electrical power, they include ROM, PROM, EPROM and EEPROM technologies. Firmware becomes “hard software” when holding program code.

Foreground: The application program currently running on and in control of the PC screen and keyboard. The area of the screen that occupies the active window. Compare with “background”.

Fractional T1 (FT1): A digital data transmission rate between 56 Kbps (DS0 rate) and 1.544M bps (the full T1 rate - in North America). FT1 is typically provided on 4-wire (two copper pairs) UTP. Often used for video conferencing, imaging and LAN interconnection due to its low cost and relatively high speed. FT1 rates are offered in 64 Kbps multiples, usually up to 768 Kbps.

Frequency: A characteristic of an electrical or electronic signal which describes the periodic recurrence of cycles. Frequency is inversely proportional to the wavelength or pulse width of the signal (i.e., long wavelength signals have low frequencies and short wavelength signals yield high frequencies).

Foreign Exchange (FX): A CO trunk with access to a distant CO, allowing ease of access and flat-rate calls anywhere in the foreign exchange area.

Foreign Exchange Office (FXO): provides local telephone service from a CO outside of (“foreign” to) the subscriber’s exchange area. In simple form, a user can pick up the phone in one city and receive a tone in the foreign city. Connecting a

POTS telephone to a computer telephony system via a T1 link requires a channel bank configured for the FX connection. To generate a call from the POTS set to the computer telephony system, a FXO connection must be configured.

Foreign Exchange Station (FXS): See FX, FXO. To generate a call from the computer telephony system to the POTS set, an FXS connection must be configured.

Forward Explicit Congestion Notification (FECN): A bit that tells you that a certain frame on a particular logical connection has encountered heavy traffic. The bit provides notification that congestion-avoidance procedures should be initiatedin the same direction of the received frame. See also BECN (Backward Explicit Congestion Notification).

Frame: A group of data bits in a specific format to help network equipment recognize what the bits mean and how to process them. The bits are sent serially, with a flag at each end signifying the start and end of the frame.

Frame Relay: A form of packet switching that uses small packets and that requires less error checking than other forms of packet switching. Frame relay is effective for sending “bursty” data at high speeds (56/64K, 256K, and 1024 Kbps) over wide area networks. Frame Relay specifications are defined by ANSI documents ANSI T1.602, T1.606, T1S1/90-175, T1S1/90-213, and T1S1/90-214. In using frame relay, blocks of information (frames) are passed across a digital network interface using a “connection number” that is applied to each frame to distinguish between individual frames.

Frame Relay Forum: A nonprofit organization of 300+ vendors and service providers, based in Foster City, CA, that are developing and deploying frame relay equipment.

Frame Relay Implementors Forum: A group of companies supporting a common specification for frame relay connection to link customer premises equipment to telco network equipment. Their specification supports ANSI frame relay specs and defines extensions such as local management.

Frame Relay Access Device (FRAD): A piece of equipment that acts as a concentrator or frame assembler/dissassembler that can support multiple protocols and provide basic “routing” functions.

G

Gateway: 1. A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. 2. A network that connects hosts.

Graphical User Interface (GUI): A type of computer interface consisting of a visual metaphor of a real-world scene, often of a desktop. Within that scene are icons, representing actual objects, that the user can access and manipulate with a pointing device.

H

Handshaking: A process that two modems go through at the time of call setup to establish synchronization over the data communications link. It is a synchronization and negotiation process accomplished by the exchange of predefined, mutually recognized control codes.

Hexadecimal: A base 16 numbering system used to represent binary values. Hex uses the numbers 0-9 and the letters A-F: usually notated by an “h” (e.g., “4CF h”, read “four charley fox, hex”). The result is that one hex digit represents a 4-bit value.

High-level Data Link Control (HDLC): An ISO standard, bit-oriented data communications protocol that provides nearly error-free data transfers.

I

Implicit congestion management: A method of informing the terminal that the network is busy. This method relies on the end-system protocol to detect and fix the congestion problem. (TCP/IP is an example of a protocol using only implicit congestion management.) See also “explicit congestion management”.

In-band: Refers to the type of signalling over the conversion path on an ISDN call. Contrast “out-of-band”.

Insufficient Ones: A T1 error condition that is logged when fewer than one 1 in 16 0s or less than 12.5 % average 1s density is received.

Inter Exchange Carrier (IEC): The long distance company (LE) who’s central office provides the point of reference for T1 access. Any common carrier authorized by the FCC to carry customer transmissions between LATAs.

Internet: Refers to the computer network of many millions of university, government and private users around the world. Each user has a unique Internet Address.

Internet Address (IP Address): A unique 32-bit address for a specific TCP/IP host on a network. Normally printed in dotted decimal format (e.g., 129.128.44.227).

Internet Protocol (IP): A protocol used to route data from its source to its destination in an Internet environment. The Internet Protocol was designed to connect local area networks. Although there are many protocols that do this, IP refers to the global system of interconnecting computers. It is a highly distributed protocol (each machine only worries about sending

data to the next step in the route).

Internetwork Packet Exchange (IPX): A NetWare communications protocol used to route messages from one node to another. IPX packets include network addresses and can be routed from one network to another. An IPX packet can occasionally get lost when crossing networks, thus IPX does not guarantee delivery of a complete message. Either the application has to provide that control, or NetWare's SPX protocol must be used.

Interoperable: Devices from different vendors that can exchange information using a standard's base protocol.

I/O Addresses: Locations within the I/O address space of your computer used by a device, such as an expansion card, a serial port, or an internal modem. The address is used for communication between software and a device.

IRQ Level (Interrupt Request Level): The notification a processor receives when another portion of the computer's hardware requires its attention. IRQs are numbered so that the device issuing the IRQ can be identified, and so IRQs can be prioritized.

ISA (Industry Standards Architecture) (pronounced "ice a"): The classic 8 or 16-bit architecture introduced with IBM's PC-AT computer.

ISDN (Integrated Services Digital Network): An International telecommunications standard for transmitting voice, video and data over a digital communications line. ISDN is a worldwide telecommunications service that uses digital transmission and switching technology to support voice and digital data communications. Frame relay was partially based on ISDN's data link layer protocol (LAPD). Frame relay can be used to transmit across ISDN services offering circuit-switched connection at 64 Kbps and higher speeds. Contrast Public Switched Telephone Network (PSTN).

ITU-TSS (formerly CCITT): International Telecommunications Union-Telecommunications Sector; the United Nations organization that prepares standards ("Recommendations") for resolving communications issues and problems.

J

No Entries.

K

Key Telephone System (KTS): Phone devices with multiple buttons that let you select incoming or outgoing CO phone lines directly. Similar in operation to a PBX, except with a KTS you don't have to dial a "9" for a call outside the building.

Key Service Unit (KSU): A small device containing the switching electronics for a business key telephone system (KTS).

Key Set: A telephone set with several buttons for call holding, line pickup, intercom, autodialing, etc. Also called a Touch-Tone phone (Ericsson) and a KTS (Key Telephone Set).

L

LAPB: Link Access Procedure Balanced; based on the X.25 Layer 2 specification. A full-duplex point-to-point, bit-synchronous protocol commonly used as a data link control protocol to interface X.25 DTEs. LAPB is the link initialization procedure that establishes and maintains communications between the DTE and the DCE.

LAPD: Link Access Protocol for the D-Channel; based on the ISDN Q.921 specification. A full-duplex, point-to-point bit-synchronous link-level protocol for ISDN connections; different from LAPB in its framing sequence. Transmission is in units called "frames", and a frame may contain one or more X.25 packets.

Line Coding: The representation of 1s and 0s on a T1 line. The two methods of line coding commonly used, B8ZS and AMI, differ in the restrictions placed on user data. T1 line coding ensures that sufficient timing information is sent with the digital signal to ensure recovery of all the bits at the far end. Timing information on the T1 line is included in the form of 1s in the data stream; a long string of 0s in the data stream could cause problems recovering the data.

Line Termination (LT): The electronics at the ISDN network side of the user/network interface that complements the NT1 at the user side. The LT and the NT1 together provide the high-speed digital line signals required for BRI access.

Listed Directory Number (LDN): The main number assigned by the telco; the number listed in the telephone directory and also provided by Directory Assistance. Some devices can have more than one LDN, such as ISDN devices that have one LDN for voice and another LDN for data.

Local Area Network (LAN): 1. A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. 2. A LAN does not use store-and-forward techniques. 3. A network in which a set of devices are connected to one another for a communication and that can be connected to a larger network.

Local Access and Transport Area (LATA): A post-divestiture geographical area generally equivalent to a Standard Metropolitan Statistical Area. At divestiture, the territory served by the Bell system was divided into approximately 161 LATAs. The Bell Operating Companies (BOCs) provide Intra-LATA services.

Local Exchange Carrier (LEC): The local phone company which provides local (i.e., not long distance) transmission services. AKA "telco". LECs provide T1 or FT1 access to LDCs (unless the T1 circuit is completely intra-LATA). Inter-LATA

T1 circuits are made up of a combination of Access and Long Haul facilities.

Local Management Interface (LMI): A specification for frame relay equipment that defines status information exchange.

Local Loop: A transmission path, typically twisted-pair wire, between an individual subscriber and the nearest public telecommunications network switching center. The wires provide ISDN service, but require an NT1 at the user end and an LT at the network end. (AKA, “loop” or “subscriber loop”.)

Logical Link Control (LLC2): In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. The LLC2 protocol was developed by the IEEE 802 commitee and is common to all LAN standards.

Logical Unit (LU): A type of network accessible unit that enables end users to gain access to network resources and communicate with each other.

Long Haul: The T1 element that connects to the Access portion of the long distance company’s (LDC’s) central office. The LDC is commonly called the point of presence (POP). Each LDC has a number of POPs, located throughout the country. The LDC is also called an IEC (Inter Exchange Carrier).

Long Haul Communications: The type of phone call reaching outside of a local exchange (LE).

M

Management Information Base (MIB): A database of network management information used by the Common Management Information Protocol (CMIP) and the Simple Network Management Protocol (SNMP).

Megacom: An AT&T service with a normal WATS line (typically T1) between the customer premise and the AT&T serving class 4 CO are the customer’s responsibility.

MegaLink: BellSouth’s leased T1 service.

Message: Associated with such terms as packet, frame, and segment. 1. In information theory, an ordered series of characters intended to convey information. 2. An assembly of characters and sometimes control codes that is transferred as an entry from an originator to one or more recipients.

Modem: A communications device that enables a computer to transmit information over a telephone line. It converts the computer’s digital signals into analog signals to send over a telephone line and converts them back to digital signals at the receiving end. Modems can be internal and fit into an expansion slot, or external and connect to a serial port.

MultiLink/PPP (ML/PPP): A ‘bandwidth on demand’ technology that allows one logical PPP connection to add additional channels (as in a second ISDN channel) when the bandwidth is needed (however the vendor defines that situation). It may also be used with leased lines when the total bandwidth needed exceeds the available line speed - a form of inverse muxing.

Multiplexer (Mux): 1. A device that takes several input signals and combines them into a single output signal in such a manner that each of the input signals can be recovered. 2. A device capable of interleaving the events of two or more activities or capable of distributing the events of an interleaved sequence to the respective activities. 3. Putting multiple signals on a single channel.

Multiprotocol: A device that can interoperate with devices utilizing different network protocols.

Multithreading: The ability of a software system to be able to handle more than one transaction concurrently. This is contrasted to the case where a single transaction is accepted and completely processed befor the next transaction processing is started.

N

Nailed Connection: A permanent or dedicated circuit of a previously switched circuit or circuits.

Nailed-up Circuit: A semipermanent circuit established through a circuit-switching facility for point-to-point connectivity.

NAK (Negative Acknowledgment): Communications code used to indicate that a message was not properly received, or that a terminal does not wish to transmit. Contrast with ACK.

Network: A group of computers connected by cables or other means and using software that enables them to share equipment, such as printers and disk drives to exchange information.

Node: Any point within a network which has been assigned an address.

O

Object-Oriented: A method for structuring programs as hierarchically organized classes describing the data and operations of objects that may interact with other objects.

Office Channel Unit - Data Port (OCU-DP): The CO channel bank used as the interface between the customer's DSU and the channel bank.

Off-hook: The condition of a device which has accessed a phone line (with or without using the line). In modem use, this is equivalent to a telephone handset being picked up. Dialing and transmission are allowed, but incoming calls are not answered. Contrast "on-hook".

Off Premise Extension (OPX): An extension or phone that terminates in a location other than that of the PBX. Commonly used to provide a corporate member with an extension of the PBX at home.

Ones Density: the measure of the number of logical 1s on a T1 line compared to a given total number of bits on that line; used for timing information in data recovery in AMI and B8ZS.

On-Hook: The condition of a device which has not accessed a phone line. In modem use, this is equivalent to a telephone handset that has not been picked up. In other words, it can receive an incoming call. Contrast "off-hook".

Open Shortest Path First (OSPF): A hierarchical Interior Gateway Protocol (IGP) routing algorithm for IP that is a proposed standard for the Internet. OSPF incorporates least-cost routing, equal-cost routing, and load balancing.

Outage: The measure of the time during which a circuit is not available for use due to service interrupt. Outage is the complement of circuit "availability" (100% minus % available = % outage).

Out-of-band: Signaling that is separated from the channel carrying the information (e.g., the voice/data/video signal is separate from the carrier signal). Dialing and various other "supervisory" signals are included in the signaling element. Contrast "In-band" signaling.

Out of Frame (OOF): A T1 alarm condition that is logged on the loss of 2, 3 or 4 of 5 consecutive FT framing bits.

P

Packet: 1. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals and, possibly, error control information are arranged in a specific format. 2. Synonymous with data frame. 3. In TCP/IP, the unit of data passed across the interface between the Internet layer and the link layer. A packet includes an IP header and data. A packet can be a complete IP datagram or a fragment of an IP diagram. 4. In X.25, a data transmission information unit. A group of data and control characters, transferred as a unit, determined by the process of transmission. Commonly used data field lengths in packets are 128 or 256 bytes. 5. The field structure and format defined in the CCITT X.25 recommendation.

Packet Assembler/Dissembler (PAD): Used by devices to communicate over X.25 networks by building or stripping X.25 information on or from a packet.

Packet Data: The information format ("packetized") used for packet-mode calls.

Packet Mode: Refers to the switching of chunks of information for different users using statistical multiplexing to send them over the same transmission facility.

Parity bit: An extra bit attached to each byte of synchronous data used to detect errors in transmission.

Password Authentication Protocol (PAP): PAP (and CHAP) are widely-used authentication methods for communicating between ProxyServers, both for reaching the Internet and for securing temporary WAN connections such as dial-backup lines. CHAP uses a three-way handshake process that, in concept, resembles a dial-back routine and uses encrypted passwords. With PAP, one ProxyServer connects to the other and sends a plain text login and password.

Permanent Virtual Circuit (PVC): A connection between two endpoints dedicated to a single user. In ISDN, PVCs are established by network administration and are held for as long as the user subscribes to the service.

Physical Unit (PU): The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only.

Point of Presence (POP): The central office's end points of the long distance carriers.

Point-to-Point Protocol (PPP): A protocol that lets a PC user access TCP/IP (Internet member) using an ISDN terminal adapter or a high-speed modem over a standard telephone line.

Port: A location for input or output data exchange. Computers, muxes, etc. have ports for various purposes.

Primary Rate Interface (PRI): Used on ISDN. In North America, and Japan, PRI is one 64 Kbps D channel and 23 B channels. Elsewhere, it is one D channel and 30 B channels.

Primitive: An abstract representation of interaction across the access points indicating that information is being passed between the service user and the service provider. The OSI Reference Model defines four types of primitives: Request, Indication, Response and Confirm.

Private Branch Exchange (PBX): A telephone exchange located on the customer's premises. The PBX provides a circuit

switching facility for telephone extension lines within the building, and access to the public telephone network. See also “Exchange”.

PROM (Programmable Read Only Memory - pronounced “prom”): A permanent memory chip that can be programmed or filled by the customer after by the manufacturer has set initial values. Contrast with ROM.

Protocol: 1. A set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. 2. In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. 3. In SNA, the meanings of and the sequencing rules for requests and responses used for managing the network, transferring data, and synchronizing the states of network components. 4. Synonymous with line control discipline.

ProxyServer: A secure gateway that provides multiple LAN users with high performance Internet access by functioning as a TCP/IP proxy server that resides on the outer edge of a firewall.

PSTN (Public Switched Telephone Network): A worldwide public voice telephone network that is used as a telecommunications medium for the transmission of voice, data and other information.

Public Data Network (PDN): A packet-switched network that is available to the public for individual (“subscriber”) use. Typically, controlled by a government or a national monopoly.

Public Switched Telephone Network (PSTN): The group of circuit-switching voice carriers, which are commonly used as analog data communications services.

Pulse Code Modulation (PCM): 1. In data communication, variation of a digital signal to represent information; for example, by means of pulse amplitude modulation (PAM), pulse duration modulation (PDM), or pulse position modulation (PPM). 2. Transmissions of analog information in digital form through sampling and encoding the samples with a fixed number of bits.

Pulse dialing: One of two methods of dialing a telephone, usually associated with rotary-dial phones. Compare with “tone dialing”.

Q

Quantizing: The process of analog-to-digital conversion by assigning a range, from the contiguous analog values, to a discrete number.

R

Random Access Memory (RAM): A computer’s primary workspace. All data must be stored in RAM (even for a short while), before software can use the processor to manipulate the data. Before a PC can do anything useful it must move programs from disk to RAM. When you turn it off, all information in RAM is lost.

Rate Enforcement: The concept in frame relay where frames sent faster than the CIR are to be carried only if the bandwidth is available, otherwise they are to be discarded. (The frame relay network assumes that anything exceeding the CIR is of low priority.) Rate enforcement makes sure that the network will not get so congested that it isn’t able to meet the agreed on CIR.

Recognized Private Operating Agency (RPOA): A corporation, private or government-controlled, that provides telecommunications services. RPOAs, such as AT&T, participate as nonvoting members in the CCITT.

Red Alarm: A T1 error condition generated when a local failure (e.g., loss of synchronization) exists for 2.5 seconds, causing a Carrier Group Alarm (CGA). See also “Blue Alarm” and “Yellow Alarm”.

Request for Comment (RFC): A set of papers in which Internet standards (published and proposed), along with generally-accepted ideas, proposals, research results, etc. are published.

Ring Down Box: A device that emulates a CO by generating POTS calls for testing and product demos.

Ring Down Circuit: A tie line connecting phones where picking up one phone automatically rings another phone. A feature used for emergencies to alert the person at the other phone of the incoming call.

RJ-11: An industry standard interface used for connecting a telephone to a modular wall outlet; comes in 4- and 6-wire packages.

RJ-45: An 8-wire modular connector for voice and data circuits.

Robbed Bit Signaling: The popular T1 signaling mechanism where the A and B bits are sent by each side of the T1 termination and are “buried” in the voice data of each voice channel in the T1 circuit. Since the bits are “robbed” infrequently, voice quality remains relatively uncompromised. See “bit robbing”. The robbed-bit signaling technique is used in D4 channel banks to convey signaling information. The eighth (least significant) bit of each of the 24 8-bit time slots is “robbed” every sixth frame to convey voice-related signaling information such as on-hook, off-hook, etc., for each channel.

Router: A device that connects two networks using the same networking protocol. It operates at the Network Layer (Layer 3) of the OSI model for forwarding decisions.

Routing Information Protocol (RIP): A distance vector-based protocol that provides a measure of distance, or hops, from a transmitting workstation to a receiving workstation.

RS232-C: An EIA standard for a serial interface between computers and peripheral devices (modem, mouse, etc.). It uses a 25-pin DB-25, or a 9-pin DB-9 connector. The RS-232 standard defines the purposes, electrical characteristics and timing of the signals for each of the 25 lines.

RS-422: The EIA standard for a balanced interface with no accompanying physical connector. RS-422 products can use screw terminals, DB9, various DB25, and DB37 connectors.

RS-530: The EIA standard for the mechanical/electrical interface between DCEs and DTEs transmitting synchronous or asynchronous serial binary data. RS-530 provides for high data rates with the same connector used for RS-232; however, it is incompatible with RS-232.

S

Serial Port: The connector on a PC used to attach serial devices (those that need to receive data one bit after another), such as a mouse, a printer or a modem. This consists of a 9- or 25-pin connector that sends data in sequence (bit by bit). Serial ports are referred to as “COMx” ports, where x is 1 to 4 (i.e., COM1 through COM4). A serial port contains a conversion chip called a “UART” which translates between internal parallel and external serial formats.

Service: The requirements offered by an RPOA to its customers to satisfy specific telecommunications needs.

Serial Line Internet Protocol (SLIP): An Internet protocol which is used to run IP over serial lines such as telephone circuits.

Severely Errored Seconds (SES): Refers to a typical T1 error event where an error burst occurs (a short term, high bit-error rate that is self-clearing). Per the ITU-T (CCITT) G.821: any second in which the BER is less than 1x10 -3 .

Signaling: The process of establishing, maintaining, accounting for, and terminating a connection between two endpoints (e.g., the user premises and the telco CO). Central office signals to the user premises can include ringing, dial tone, speech signals, etc. Signals from the user’s telephone can include off-hook, dialing, speech to far-end party, and on-hook signals. In-band signaling techniques include pulse and tone dialing. With common channel signaling, information is carried out-of-band.

Simple Network Management Protocol (SNMP): TCP/IP protocol that allows network management.

Simultaneous Voice Data (SVD): A technology for letting a user send data via a modem, and use a handset to talk to another user at the same time over the same connection. The alternative, making a second call, can be expensive or even impossible. The uses for SVD are telecommuting, videoconferencing, distant learning, tech support, etc.

Stop Bit: One of the variables used for timing in asynchronous data transmission. Depending on the devices, each character may be trailed by 1, 1.5, or 2 stop bits.

Superframe (D4): A T1 transmission format that consists of 12 DS1 frames, or 2316 bits. A DS1 frame consists of 193 bit positions. A frame overhead bit is in the first position, and it is used for frame and signaling phase alignment only.

Subscriber Loop: See “Local loop”.

Switched 56: A circuit-switched (full duplex digital synchronous data transmission) service that lets you dial a number and transmit data to it at 56 Kbps. It is a relatively low cost service, widely used in North America for telecommuting, videoconferencing and high speed data transfers. Many phone companies are (or will be) phasing out Switched 56 in favor of ISDN service.

Switched Virtual Circuit (SVC): A type of data transmission where the connection is maintained only until the call is cleared.

Switched Line: In communications, a physical channel established by dynamically connecting one or more discrete segments. This connection lasts for the duration of the call after which each segment can be used as part of a different channel. Contrast with leased line.

Switched Network: A network in which a temporary connection is established from one point via one or more segments.

Synchronous Data Link Control (SDLC): A discipline conforming to subsets of the Advanced Data Communications Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex, or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop.

Synchronous Transmission: The transmission of data which involves sending a group of characters in a packet. This is a common method of transmission between computers on a network or between modems. One or more synchronous characters are transmitted to confirm clocking before each packet of data is transmitted. Compare to Asynchronous Transmission.

Systems Network Architecture (SNA): The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of networks.

T

Tariff: The rate/availability schedule for telephone and ISDN services from a regulated service provider.

TCP/IP: A set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks.

T Carrier: The generic name for a digitally multiplexed carrier system. In the North American digital hierarchy, a T is used to designate a DS (digital signal) level hierarchy. Examples: T1 (DS1) is a 1.544 Mbps 24-channel designation. In Europe, T1 is called E1. The T Carrier system was originally designed for transmitting digitized voice signals, but has since been adapted for digital data applications.

T1: A digital transmission link capable of 1.544 Mbps. T1 uses two pairs of normal UTP, and can handle 24 voice conversations, each digitized at 64 Kbps. T1 is a standard for digital transmission in the U.S., Canada, Japan and Hong Kong. T1 is the access method for high-speed services such as ATM, frame relay, and SMDS. See also T Carrier, T1 line and FT1.

T1 Channel Tests: A set of diagnostics that varies by carrier, used to verify a T1 channel operation. Can include Tone, Noise Level, Impulse Noise Level, Echo Cancelers, Gain, and Crosstalk testing.

T1 Framing: To digitize and encode analog voice signals requires 8000 samples per second (twice the highest voice frequency of 4000 Hz). Encoding in an 8-bit word provides the basic T1 block of 64 Kbps for voice transmission. This “Level 0 Signal, as its called, is represented by “DS-0”, or Digital Signal at Level 0. 24 of these voice channels are combined into a serial bit stream (using TDM), on a frame-by-frame basis. A frame is a sample of all 24 channels; so adding in a framing bit gives a block of 193 bits (24x8+1=193). Frames are transmitted at 8000 per second (the required sample rate), creating a 1.544M (8000x193=1.544M) transmission rate.

T1 Line: A digital communications facility that functions as a 24-channel pathway for data or voice transmission. A T1 line is composed of two separate elements: the Access element and the Long Haul element.

T1 Mux: A device used to carry many sources of data on a T1 line. The T1 mux assigns each data source to distinct DS0 time slots within the T1 signal. Wide bandwidth signals take more than one time slot. Normal voice traffic or 56/64 Kbps data channels take one time slot. The T1 mux may use an internal or external T1 DSU; a “channel bank” device typically uses an external T1 CSU.

Transmission Control Protocol / Internet Program (TCP/IP): A multilayer set of protocols developed by the US Department of Defense to link dissimilar computers across dissimilar and unreliable LANs.

Terminal: The screen and keyboard device used in a mainframe environment for interactive data entry. Terminals have no “box”, which is to say they have no file storage or processing capabilities.

Terminal Adapter (TA): An ISDN DTE device for connecting a non-ISDN terminal device to the ISDN network. Similar to a protocol converter or an interface converter, a TA connects a non-ISDN device between the R and S interfaces. Typically a PC card.

Terminal Endpoint Identifier (TEI): Up to eight devices can be connected to one ISDN BRI line. The TEI defines for a given message which of the eight devices is communicating with the Central Office switch. In general, more than one of the eight may be communicating.

Tie line: A dedicated circuit linking two points without having to dial a phone number (i.e., the line may be accessed by lifting the telephone handset or by pushing a button).

Time-Division Multiplexing (TDM): Division of a transmission facility into two or more channels by allotting the common channel to several different information channels, one at a time.

Time Slot: One of 24 channels within a T1 line. Each channel has a 64 Kbps maximum bandwidth. “Time slot” implies the time division multiplexing organization of the T1 signal.

Toll Call: A call to a location outside of your local service area (i.e., a long distance call).

Tone dialing: One of two methods of dialing a telephone, usually associated with Touch-Tone® (push button) phones. Compare with pulse dialing.

Topology: Physical layout of network components (cables, stations, gateways, and hubs). Three basic interconnection topologies are star, ring, and bus networks.

Transmission Control Protocol (TCP): A communications protocol used in Internet and in any network that follows the US Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It assumes that the Internet protocol is the underlying protocol.

Transport Layer: Layer 4 of the Open Systems Interconnection (OSI) model; provides reliable, end-to-end delivery of data, and detects transmission sequential errors.

Transport Protocol Data Unit (TPDU): A transport header, which is added to every message, contains destination and source addressing information that allows the end-to-end routing of messages in multilayer NAC networks of high

complexity. They are automatically added to messages as they enter the network and can be stripped off before being passed to the host or another device that does not support TPDU's.

Trunk: Transmission links that interconnect switching offices.

TSR (terminate and stay resident): A software program that remains active and in memory after its user interface is closed. Similar to a daemon in UNIX environments.

Tunneling: Encapsulation data in an IP packet for transport across the Internet.

Twisted pair wiring: A type of cabling with one or more pairs of insulated wires wrapped around each other. An inexpensive wiring method used for LAN and telephone applications, also called UTP wiring.

U

UART (Universal Asynchronous Receiver/Transmitter) (pronounced "you art"): A chip that transmits and receives data on the serial port. It converts bytes into serial bits for transmission, and vice versa, and generates and strips the start and stop bits appended to each character.

UNIX: An operating system developed by Bell Laboratories that features multiprogramming in a multi-user environment.

Unshielded Twisted Pair (UTP): Telephone-type wiring. Transmission media for 10Base-T.

User Datagram Protocol (UDP): A TCP/IP protocol describing how messages reach application programs within a destination computer. This protocol is usually bundled with IP-layer software. UDP is a transport layer, connectionless mode protocol, providing a (potentially unreliable, unsequenced, and/or duplicated) datagram mode of communication for delivery of packets to a remote or local user.

V

V.25bis: An ITU-T standard for synchronous communications between a mainframe or host and a modem using HDLC or other character-oriented protocol.

V.54: The ITU-T standard for local and remote loopback tests in modems, DCEs and DTEs. The four basic tests are:

- local digital loopback (tests DTE send and receive circuits),
- local analog loopback (tests local modem operation),
- remote analog loopback (tests comm link to the remote modem), and
- remote digital loopback (tests remote modem operation).

Virtual Circuit: A logical connection. Used in packet switching wherein a logical connection is established between two devices at the start of transmission. All information packets follow the same route and arrive in sequence (but do not necessarily carry a complete address).

W

Wide Area Network (WAN): 1. A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. 2. A data communications network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. Contrast with local area network (LAN).

Wide Area Telecommunications Service (WATS): A low-cost toll service offered by most long distance and local phone companies. Incoming (800 call service, or IN-WATS) and outgoing WATS are subscribed to separately, but over the same line.

X

X.25: ITU-T's definition of a three-level packet-switching protocol to be used between packet-mode DTEs and network DCEs. X.25 corresponds with layer 3 of the 7-layer OSI model.

Y

Yellow Alarm: An error indication sent by the T1 device when it has not gotten a receive signal, or cannot synchronize on the receive signal received. Contrast "Red Alarm" and "Blue Alarm".

Z

Zero Byte Time Slot Interchange (ZBTSI): A method for allowing 64 Kbps unrestricted user data (allowing all 0s in the user data). An alternative to (but not as popular as) B8ZS.

Index

A

Accessories, ordering 83
Adding Proxy Applications 38
Applications 38
Archie 87

B

Back Panel 9
  Connectors 9

C

Cabinet Mounting Screw 17
Cabling Your ProxyServer 18
Changing IP Parameters 32
Changing WAN Port Parameters 35
Client Setup 50
  Configuring in Windows 95/98 51
  Configuring in Windows NT 59
  Installing TCP/IP (Win95/98) 58
  Installing TCP/IP (WinNT) 65
  Overview 50
Command Connector 9
Configuration Port Setup 30
Configuration Utilities 30
Connectors 9
  10Base-T 9
  Command 9
  Ethernet 1 and 2 9
  Power 9
  RS232/V.35 9

D

Data Communications Equipment 9
DCE. *See* Data Communications Equipment
DHCP Client 32
DHCP Relay Agent 32
DHCP Server 37
DNS 87
Download Firmware 30

E

Enabling the DHCP Server 37
Ethernet 1 and 2 Connectors 9

F

Finger 87
Firewall Configuration 31
Front Panel 8
  LEDs 8
FTP 87

G

Gopher 87

H

HTML 87
HTTP 87

I

Installing TCP/IP (Win95/98) 58
Installing TCP/IP (WinNT) 65
Internet 83
Internet Gateway Parameters 33
Internet LAN Port Parameters 32
Internet Protocol 86, 88
Internet Services Network 6
IP 88
IP Parameters 32

L

LEDs 8
  ETHERNET 1 and 2 8
  Fail 8
  Power 8
  WAN Link 8
Limited Warranty 80
Loading Your Software 22

M

MTPSR3-200
  Accessories, ordering 83

O

On-line Warranty Registration 80
Ordering accessories 83

P

Ping 87
POP 87
Power Connector 9
Proxy Applications 38
ProxyServer program group 30

ProxyServer Telnet server menu 75
Whois/NICNAME 87

R

Regulatory information
EMC and safety directive compliance 93
RS232/V.35 Connector 9

S

Safety Warnings 16
Scripting
Commands (by function) 91
Example script 92
Secured LAN Port Parameters 32
Service 82
Shunt Positions 17
SMTP 87
SNMP 87
Software
Applications 38
DHCP Server 37
Firewall Configuration 31
IP Parameters 32
Proxy Applications 38
WAN Port Parameters 35
Specifications 11

T

TCP/IP 86
Tech Support 81
Technical Specifications 11
Telnet 87
Client 74
Traceroute 87
Transmission Control Protoco 86
Typical Applications
Configuration 1 - Cable/DSL Modem 10
Configuration 2 - Existing Dual-LAN with Router 11
Configuration 3 - New Dual-LAN with T1 DSU 12

U

Uninstall Proxy Server Configuration 30
Unpacking Your ProxyServer 16

V

Virtual server, setup 41

W

WAN Device Configuration 30
WAN Port Parameters 33, 35
Warranty 80
On-line Warranty Registration 80